Tenable.io Report

Tenable.io Report

Mon, 13 Feb 2023 02:44:05 UTC

Table Of Contents

Vulnerabilities By Host

security-aig-301.itest.conn.com

Scan Information

Start time: 2023/02/13 02:07

End time: 2023/02/13 02:44

Host Information

DNS Name: security-aig-301.itest.conn.com

OS: [0: Linux Kernel 4.4.0-cip-rt-moxa-imx7d-aig-301 on Debian 9.13]

Results Summary

Critical	High	Medium	Low	Info	Total
1	3	3	0	63	70

Results Details

/

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2002/03/06, Modification date: 2021/01/19

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/08/19, Modification date: 2022/07/26

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
An SSH server is running on this port.
```

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
A TLSv1.2 server answered on this port.


A web server is running on this port through TLSv1.2.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
Local checks have been enabled.
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/05/23, Modification date: 2022/09/09

Ports
security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 100
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/06/30, Modification date: 2023/02/06

Ports
security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Hostname : Moxa
  Moxa (hostname command)
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/10/12, Modification date: 2018/06/19

Ports
security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
reboot   system boot  4.4.0-cip-rt-mox Mon Feb 13 09:52   still running

wtmp begins Mon Feb 13 09:52:34 2023
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
SHA384
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA       Camellia-CBC(128)
SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA       Camellia-CBC(256)
SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA       AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/07/02, Modification date: 2021/05/19

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

100158 - SSH Combined Host Command Logging (Plugin Debugging)

Synopsis

If plugin debugging is enabled, this plugin writes the SSH commands run on the host to a combined log file in a machine readable format.

Description

If plugin debugging is enabled, this plugin writes the SSH commands run on the host to a combined log file in a machine readable format.
This log file resides on the scanner host itself.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/05/12, Modification date: 2022/11/21

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Combined log file location :

  C:\ProgramData\Tenable\Nessus\nessus\tmp\ssh_commands-8be03e7c-4c74-49bb-aed9-394d33f212a1.log
```

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

See Also

Solution

N/A

Risk Factor

None

References

XREF IAVB:0001-B-0502

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/06/06, Modification date: 2021/07/26

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User:       'moxa'
Port:       22
Proto:      SSH
Method:     password


See the output of the following plugin for details :

  Plugin ID   : 102094
  Plugin Name : SSH Commands Require Privilege Escalation
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/06/12, Modification date: 2022/06/29

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
 USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  1.1  0.2  25896  5608 ?        Ss   09:51   0:28 /sbin/init
root          2  0.0  0.0      0     0 ?        S    09:51   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    09:51   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S<   09:51   0:00 [kworker/0:0H]
root          6  0.6  0.0      0     0 ?        S    09:51   0:16 [kworker/u4:0]
root          7  0.2  0.0      0     0 ?        S    09:51   0:06 [rcu_sched]
root          8  0.0  0.0      0     0 ?        S    09:51   0:00 [rcu_bh]
root          9  0.4  0.0      0     0 ?        S    09:51   0:11 [rcuc/0]
root         10  0.0  0.0      0     0 ?        S    09:51   0:00 [migration/0]
```

```
root         11  0.0  0.0      0     0 ?        S    09:51   0:00 [migration/1]
root         12  0.4  0.0      0     0 ?        S    09:51   0:09 [rcuc/1]
root         13  0.0  0.0      0     0 ?        S    09:51   0:00 [ksoftirqd/1]
root         15  0.0  0.0      0     0 ?        S<   09:51   0:00 [kworker/1:0H]
root         16  0.0  0.0      0     0 ?        S    09:51   0:00 [kdevtmpfs]
root         17  0.0  0.0      0     0 ?        S<   09:51   0:00 [netns]
root         18  0.0  0.0      0     0 ?        S    09:51   0:00 [kswork]
root         19  0.0  0.0      0     0 ?        S<   09:51   0:00 [perf]
root         20  0.0  0.0      0     0 ?        S<   09:51   0:00 [writeback]
root         21  0.0  0.0      0     0 ?        S<   09:51   0:00 [crypto]
root         22  0.0  0.0      0     0 ?        S<   09:51   0:00 [bioset]
root         23  0.0  0.0      0     0 ?        S<   09:51   0:00 [kblockd]
root         24  0.0  0.0      0     0 ?        S<   09:51   0:00 [ata_sff]
root         25  0.0  0.0      0     0 ?        S<   09:51   0:00 [watchdogd]
root         26  0.0  0.0      0     0 ?        S<   09:51   0:00 [rpciod]
root         29  0.0  0.0      0     0 ?        S    09:51   0:00 [kswapd0]
root         30  0.0  0.0      0     0 ?        S<   09:51   0:00 [...]
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/10/02, Modification date: 2021/07/12

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
OS Security Patch Assessment is available.

Account  : moxa
Protocol : SSH
```

118151 - nginx Data Disclosure Vulnerability

Synopsis

The remote web server is affected by a data disclosure vulnerability.

Description

According to its Server response header, the installed version of nginx is prior to 1.12.1 or 1.13.x prior to 1.13.3. It is, therefore, affected by an integer overflow vulnerability in the range filter module. An unauthenticated, remote attacker can exploit this, via a specially crafted request to disclose potentially sensitive information.

See Also

http://nginx.org/en/security_advisories.html

http://mailman.nginx.org/pipermail/nginx-announce/2017/000200.html

Solution

Either apply the patch manually or upgrade to nginx 1.12.1 / 1.13.3 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2017-7529
BID	103938

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2018/10/16, Modification date: 2022/04/11

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Installed version : 1.10.3
Fixed version     : 1.12.1 / 1.13.3
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.
Please note the following :
- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/10/15, Modification date: 2021/07/26

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Active

```
Nessus was able to log in to the remote host via the following :

User:       'moxa'
Port:       22
Proto:      SSH
Method:     password
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/05/07, Modification date: 2021/05/07

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

22869 - Software Enumeration (SSH)

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

See Also

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT:0001-T-0502

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/10/15, Modification date: 2022/09/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Here is the list of packages installed on the remote Debian Linux system :

  ii   adduser  3.115  all  add and remove users and groups
  ii   aig-301-base-system  1.5.5  armhf  Base system for AIG-301
  ii   aig-301-kernel  4.4.285-cip63-rt36-moxa15-aig-301-4+deb9  armhf  i.MX7 Flattened Image
  ii   aig-301-modules  4.4.285-cip63-rt36-moxa15-aig-301-4+deb9  armhf  i.MX7 standard kernel
 modules
  ii   apache2  2.4.25-3+deb9u12  armhf  Apache HTTP Server
  ii   apache2-bin  2.4.25-3+deb9u12  armhf  Apache HTTP Server (modules and other binary files)
  ii   apache2-data  2.4.25-3+deb9u12  all  Apache HTTP Server (common files)
  ii   apache2-utils  2.4.25-3+deb9u12  armhf  Apache HTTP Server (utility programs for web
 servers)
  hi   appman  2.3.0-2553  armhf  App Manager for Moxa ThingsPro Edge
  ii   apt  1.4.11  armhf  commandline package manager
  ii   apt-utils  1.4.11  armhf  package management related utility programs
  ii   aziot-edge  1.2.7-1  armhf  Azure IoT Edge Module Runtime
  ii   aziot-identity-service  1.2.5-1  armhf  Azure IoT Identity Service and related services
  ii   base-files  9.9+deb9u13  armhf  Debian base system miscellaneous files
  ii   base-passwd  3.5.43  armhf  Debian base system master password and group files
  ii   bash  4.4-5  armhf  GNU Bourne Again SHell
  ii   bc  1.06.95-9+b3  armhf  GNU bc arbitrary precision calculator language
  ii   bsdmainutils  9.0.12+nmu1  armhf  collection of more utilities from FreeBSD
  ii   bsdutils  1:2.29.2-1+deb9u1  armhf  basic utilities from 4.4BSD-Lite
  ii   busybox  1:1.22.0-19+deb9u2  armhf  Tiny utilities for small and embedded systems
  ii   ca-certificates  20200601~deb9u2  all  Common CA certificates
  ii   can-utils  0.0+git20161220-1  armhf  SocketCAN userspace utilities and tools
  ii   cgmanager  0.41-2  armhf  Central cgroup manager daemon
  ii   coreutils  8.26-3  armhf  GNU core utilities
  ii   cpio  2.11+dfsg-6  armhf  GNU cpio -- a program to manage archives of files
  ii   crda  3.18-1  armhf  wireless Central Regulatory [...]
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/08/08, Modification date: 2023/02/07

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Debian 9.13 support ended on 2020-07-06 (end of regular support) / 2022-06-30 (end of long-term
 support for Stretch-LTS).
Upgrade to Debian Linux 10.x ("Buster").

For more information, see : http://www.debian.org/releases/


Debian 9.13 support ended on 2020-07-06 (end of regular support) / 2022-06-30 (end of long-term
 support for Stretch-LTS).
Upgrade to Debian Linux 10.x ("Buster").

For more information, see : http://www.debian.org/releases/

Debian 9.1 support ended on 2020-07-06 (end of regular support) / 2022-06-30 (end of long-term
 support for Stretch-LTS).
Upgrade to Debian Linux 10.x ("Buster").

For more information, see : http://www.debian.org/releases/
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

See Also

Solution

Disable IPv6 if you do not actually using it.
Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/04/02, Modification date: 2012/08/07

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following global addresss were gathered :

  - ['ipv6': fe80::42:eaff:fe77:6e92]['prefixlen': 64]
  - ['ipv6': fe80::290:e8ff:fe8f:ef7c]['prefixlen': 64]
  - ['ipv6': ::1]['prefixlen': 128]
  - ['ipv6': fe80::d4d7:5fff:fe82:be70]['prefixlen': 64]
  - ['ipv6': fe80::c850:4dff:fe3b:e033]['prefixlen': 64]
  - ['ipv6': fe80::5865:5dff:fea6:ca78]['prefixlen': 64]
  - ['ipv6': fe80::c038:1ff:fe85:837f]['prefixlen': 64]
  - ['ipv6': fe80::9470:42ff:fe07:9471]['prefixlen': 64]
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.
The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

https://content-security-policy.com/

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/10/26, Modification date: 2021/01/19

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://security-aig-301.itest.conn.com:8443/
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
```

```
The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/07/17, Modification date: 2021/02/03

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
http/1.1
```

90707 - SSH SCP Protocol Detection

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/04/26, Modification date: 2017/08/28

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Active

102094 - SSH Commands Require Privilege Escalation

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.
NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVB:0001-B-0507

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/08/01, Modification date: 2020/09/22

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Login account : moxa
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
  Escalation method  : (none)
  Plugins :
  - Plugin Filename : apache_http_server_nix_installed.nbin
    Plugin ID       : 141394
    Plugin Name     : Apache HTTP Server Installed (Linux)
    - Command  : "grep -aE '(Oracle-HTTP-Server)' /var/log/apache2 2>&1"
      Response : "grep: /var/log/apache2: Permission denied"
      Error    : ""
    - Command  : "grep -aE '.*(Apache\\/([0-9][0-9]?\\.[0-9][0-9]?\\.[0-9][0-9]?) \\([A-Za-z ]*\
\)).*' /var/log/apache2 2>&1"
      Response : "grep: /var/log/apache2: Permission denied"
      Error    : ""
  - Plugin Filename : host_tag_nix.nbin
    Plugin ID       : 87414
    Plugin Name     : Host Tagging (Linux)
    - Command  : "sh -c \"echo 58f1ee29cf8b406f90b0659644e3048c > /etc/tenable_tag && echo OK\""
      Response : null
      Error    : "sh: 1: \ncannot create /etc/tenable_tag: Permission denied"
  - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
    Plugin ID       : 125216
    Plugin Name     : Processor Speculative Execution Vulnerabilities (Linux)
    - Command  : "cat /sys/kernel/debug/x86/pti_enabled"
      Response : null
      Error    : "cat: /sys/kernel/debug/x86/pti_enabled: Permission denied"
    - Command  : "cat /sys/kernel/debug/x86/retp_enabled"
      Response : null
      Error    : "cat: /sys/kernel/debug/x86/retp_enabled: Permission denied"
    - Command  : "cat /sys/kernel/debug/x86/ibrs_enabled"
      Response : null
      Error    : "cat: \n/sys/kernel/debug/x86/ibrs_enabled\n: Permission denied"
  - Plugin Filename : localusers_pwexpiry.nasl
    Plugin ID       : 83303
    Plugin Name     : Unix / Linux - Local Users Information : Passwords Never Expire
    - Command  : "cat /etc/shadow"
      Response : null
      Error    : "cat: \n/etc/shadow\n: Permission denied"
  - Plugin Filename : unix_compliance_check.nbin
    Plugin ID       : 21157
    Plugin Name     : Unix Compliance Checks
    - Command  : "LANG=C; [...]
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/05/04, Modification date: 2020/05/04

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

142640 - Apache HTTP Server Site Enumeration

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

https://httpd.apache.org/

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/11/09, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Sites and configs present in /usr/sbin/apache2 Apache installation:
  - following sites are present in /etc/apache2/apache2.conf Apache config file:
    +  - *:80
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

See Also

Solution

Protect your target with an IP filter.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/04, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
Port 22/tcp was found to be open
```

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
Port 8443/tcp was found to be open
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/12/09, Modification date: 2022/03/09

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Remote operating system : Linux Kernel 4.4.0-cip-rt-moxa-imx7d-aig-301 on Debian 9.13
Confidence level : 100
Method : LinuxDistribution

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:!:SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
uname:Linux Moxa 4.4.0-cip-rt-moxa-imx7d-aig-301 #1 SMP Wed Jul 13 15:11:31 CST 2022 armv7l GNU/
Linux

SinFP:!:
   P1:B10113:F0x12:W29200:O0204ffff:M1460:
   P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190402_7_p=22R
SSLcert:!:i/CN:ThingsPro Edge Root CA for HTTPSi/O:Moxa Inc.s/CN:ThingsPro Edge Gateway
 Certificate for HTTPSs/O:Moxa Inc.
34c1f6c9699a3d60948af1a49079321a029900de



The remote host is running Linux Kernel 4.4.0-cip-rt-moxa-imx7d-aig-301 on Debian 9.13
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
172.16.2.216 resolves as security-aig-301.itest.conn.com.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2005/08/26, Modification date: 2022/06/09

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.4.2
Nessus build : 20093
Plugin feed version : 202302120407
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : ThingsPro Edge - DevOps
Scan policy used : MOXA Default (IBG)
Scanner IP : 192.168.0.160
Port scanner(s) : nessus_syn_scanner
Port range : all
Ping RTT : 15.628 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : yes (at debugging level 4)
Paranoia level : 1
Report verbosity : 1
Safe checks : no
Optimize the test : yes
```

```
Credentialed checks : yes, as 'moxa' via ssh
Attempt Least Privilege : yes
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2023/2/13 10:08 Taipei Standard Time
Scan duration : 2000 sec
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/06/05, Modification date: 2022/07/25

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code              KEX           Auth     Encryption
 MAC
   ----------------------        ----------        ---           ----     --------------------
 ---
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA      Camellia-CBC(128)
 SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA      Camellia-CBC(256)
 SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C        RSA           RSA      AES-CCM(128)
 AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0        RSA           RSA      AES-CCM8(128)
 AEAD
   RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA      AES-GCM(128)
 SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D        RSA           RSA      AES-CCM(256)
 AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1        RSA           RSA      AES-CCM8(256)
 AEAD
```

```
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA          [...]
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

See Also

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/11, Modification date: 2022/02/23

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following IPv6 interfaces are set on the remote host :

 - fe80::42:eaff:fe77:6e92 (on interface br-db93bafdc65d)
 - fe80::290:e8ff:fe8f:ef7c (on interface eth0)
 - ::1 (on interface lo)
 - fe80::d4d7:5fff:fe82:be70 (on interface veth8b0dfc3)
 - fe80::c850:4dff:fe3b:e033 (on interface vethb3c47cf)
 - fe80::9470:42ff:fe07:9471 (on interface vethbe34269)
 - fe80::c038:1ff:fe85:837f (on interface vethc22aed9)
 - fe80::5865:5dff:fea6:ca78 (on interface vethc7e1984)
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. However, this is assuming there are no intermediate devices between the scanner and the target. Firewalls often block ICMP, which will prevent responses that identify closed ports. The scanning primarily relies on the absence of a response to identify open ports and in complex environments with many intermediate devices, the detection can often be unreliable.
UDP scanning takes a long time to complete. The scanner must limit the number of concurrent probes because ICMP is often rate limited. Also, since open ports do not respond, the scanner must wait for a timeout period to be reasonably sure that no response will be received.
Given the typical environments being scanned today, the results of this plugin should be thoroughly vetted and be used as weak signals for further investigation. It is likely that a large number of assets will be detected if there are intermediate devices between the scanner and the targets. Consider using the netstat or SNMP port enumeration options instead if possible.

See Also

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/04, Modification date: 2023/02/10

Ports

security-aig-301.itest.conn.com (UDP/0) Vulnerability State: Active

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/04/21, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :

  cpe:/o:debian:debian_linux:9.13 -> Debian Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.25 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:log4j -> Apache Software Foundation log4j
  cpe:/a:gnupg:libgcrypt:1.8.4 -> GnuPG Libgcrypt
  cpe:/a:nginx:nginx:1.10.3 -> Nginx
  cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.1.0l -> OpenSSL Project OpenSSL
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/12/15, Modification date: 2020/04/27

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : ST=Taiwan/L=New Taipei City/O=Moxa Inc./CN=ThingsPro Edge Gateway Certificate for
 HTTPS
|-Issuer  : ST=Taiwan/L=New Taipei City/O=Moxa Inc./CN=ThingsPro Edge Root CA for HTTPS
```

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections. Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

https://technotes.googlecode.com/git/nextprotoneg.html

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2012/10/16, Modification date: 2022/04/11

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The target advertises that the following protocols are
supported over SSL / TLS:

  http/1.1
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/10/16, Modification date: 2020/05/13

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following is a consolidated list of detected MAC addresses:
  - 00:90:E8:8F:EF:7D
  - 5A:65:5D:A6:CA:78
  - 02:42:EA:77:6E:92
  - 9E:21:95:88:B2:90
  - D6:D7:5F:82:BE:70
  - 00:0E:8E:9C:8B:B2
  - 02:42:95:39:D5:4D
  - 96:70:42:07:94:71
  - C2:38:01:85:83:7F
  - CA:50:4D:3B:E0:33
  - 00:90:E8:8F:EF:7C
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote host.

See Also

Solution

None

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/12/19, Modification date: 2022/06/29

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
----------[ User Accounts ]----------

User         : moxa
Home folder  : /home/moxa
Start script : /bin/bash
Groups       : moxa
               iotedge
               sudo

User         : tss
Home folder  : /var/lib/tpm
Start script : /bin/false
Groups       : tss

User         : redis
Home folder  : /var/lib/redis
Start script : /bin/false
Groups       : redis

User         : mosquitto
Home folder  : /var/lib/mosquitto
Start script : /usr/sbin/nologin
Groups       : mosquitto

User         : aziotks
Home folder  : /var/lib/aziot/keyd
Start script : /sbin/nologin
Groups       : aziotks

User         : aziottpm
Home folder  : /var/lib/aziot/tpmd
Start script : /sbin/nologin
Groups       : aziottpm

User         : aziotcs
Home folder  : /var/lib/aziot/certd
Start script : /sbin/nologin
Groups       : aziotcs
               aziotks

User         : aziotid
Home folder  : /var/lib/aziot/identityd
Start script : /sbin/nologin
Groups       : aziottpm
               aziotcs
               aziotks
               aziotid

User         : iotedge
Home folder  : /var/lib/aziot/edged
Start script : /sbin/nologin
Groups       : iotedge
               systemd-journal
               aziotcs
               aziotks
               docker
               aziotid

----------[ System Accounts ]----------

User         : root
Home folder  : /root
```

```
Start script : /bin/bash
Groups       : root

User         : daemon
Home folder  : /usr/sbin
Start script : /usr/sbin/nologin
Groups       : daemon

User         : bin
Home folder  : /bin
Start script : /usr/sbin/nologin
Groups       : bin

User         : sys
Home folder  : /dev
Start script : /usr/sbin/nologin
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

User         : games
Home folder  : /usr/games
Start script : /usr/sbin/nologin
Groups       : games

User         : man
Home folder  : /var/cache/man
Start script : /usr/sbin/nologin
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : [...]
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/05/30, Modification date: 2021/08/02

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
It was possible to log into the remote host via SSH using 'password' authentication.

Local checks have been enabled for this host.
The remote Debian system is :
9.13

OS Security Patch Assessment is available for this host.
Note, though, that an attempt to elevate privileges using 'su+sudo' failed
for an unknown reason. Further commands will be run as the user
specified in the scan policy.
```

```
Runtime : 13.575494 seconds
```

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/07/21, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /lib/arm-linux-gnueabihf/libgcrypt.so.20
  Version : 1.8.4

  Path    : /lib/arm-linux-gnueabihf/libgcrypt.so.20.2.4
  Version : 1.8.4
```

152743 - Unix Software Discovery Commands Not Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.
Details of the issues encountered are reported by this plugin.
Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.
Commands used to find unmanaged software installations might fail for a variety of reasons, including:
* Inadequate scan user permissions,
* Failed privilege escalation,
* Intermittent network disruption, or
* Missing or corrupt executables on the target host.
Please address the issues reported here and redo the scan.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/08/23, Modification date: 2021/08/23

Ports
security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Failures in commands used to assess Unix software:

  unzip -v                    :
    bash: unzip: command not found


Account  : moxa
Protocol : SSH
```

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.
/bin/df -h /bin/lsblk /bin/mount -l
This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/02/03, Modification date: 2022/09/08

Ports
security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
 $ df -h
Filesystem          Size  Used Avail Use% Mounted on
devtmpfs           1005M     0 1005M   0% /dev
tpmfs              1010M  5.4M 1004M   1% /run
/dev/mmcblk2p2      645M  475M  124M  80% /boot_device/p2
/dev/loop0          474M  474M     0 100% /boot_device/p2/lower
/dev/mapper/crypto   14G  3.3G   10G  25% /boot_device/p3
overlay              14G  3.3G   10G  25% /
/dev/mmcblk2p1       54M   33M   18M  66% /boot_device/p1
tmpfs              1010M     0 1010M   0% /dev/shm
tmpfs               5.0M     0  5.0M   0% /run/lock
tmpfs              1010M     0 1010M   0% /sys/fs/cgroup
tmpfs               202M     0  202M   0% /run/user/1000


$ lsblk
NAME         MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
loop0          7:0    0 473.2M  0 loop  /boot_device/p2/lower
mtdblock0     31:0    0     1M  0 disk
mtdblock1     31:1    0     1M  0 disk
mtdblock2     31:2    0     1M  0 disk
mtdblock3     31:3    0   128K  0 disk
mtdblock4     31:4    0   128K  0 disk
mtdblock5     31:5    0     1M  0 disk
mmcblk0      179:0    0  29.7G  0 disk
 └─mmcblk0p1 179:1    0  29.7G  0 part
mmcblk2      179:8    0  14.8G  0 disk
 ├─mmcblk2p1 179:9    0    64M  0 part  /boot_device/p1
 ├─mmcblk2p2 179:10   0   663M  0 part  /boot_device/p2
 └─mmcblk2p3 179:11   0  14.1G  0 part
   └─crypto   254:0    0  14.1G  0 crypt /boot_device/p3
```

```
mmcblk2boot0 179:16   0  31.5M  1 disk
mmcblk2boot1 179:24   0  31.5M  1 disk
mmcblk2rpmb  179:32   0     4M  0 disk


$ mount -l
devtmpfs on /dev type devtmpfs (rw,relatime,size=1028420k,nr_inodes=186531,mode=755)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
tpmfs on /run type tmpfs (rw,relatime)
/dev/mmcblk2p2 on /boot_device/p2 type ext4 (rw,relatime,data=ordered)
/dev/loop0 on /boot_device/p2/lower type squashfs (ro,relatime)
/dev/mapper/crypto on /boot_device/p3 type ext4 (rw,relatime,data=ordered)
overlay on / type overlay [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/01/30, Modification date: 2019/11/22

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Mon, 13 Feb 2023 02:35:16 GMT
  Content-Type: text/html
  Content-Length: 2386
  Last-Modified: Mon, 23 May 2022 07:32:56 GMT
  Connection: keep-alive
  Vary: Accept-Encoding
  ETag: "628b38a8-952"
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block
  Cache-Control: no-cache
  Accept-Ranges: bytes

Response Body :

<!DOCTYPE html><html lang="en"><head>
    <meta charset="utf-8">
    <title>ThingsProÃ® Edge</title>
    <base href="/">

    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="icon" type="image/x-icon" href="favicon.ico">
```

```
  <style>@import"https://fonts.googleapis.com/css?
family=Roboto:300,400,500&display=swap";html{line-height:1.15;-webkit-text-size-
adjust:100%}body{margin:0}html,body{letter-spacing:.015em;margin:0;height:100%;font-
family:Roboto,sans-serif;font-weight:400}.square{width:100%;height:100%;display:flex;justify-
content:center;align-items:center}.spinner-circular__index-
page{box-sizing:border-box;width:100px;height:100px}@keyframes
 spinnerCircularAnimate{0%{transform:rotate(0)}to{transform:rotate(360deg)}}.square{width:100%;height:100%;dis
content:center;align-items:center}.spinner-circular__index-
page{box-sizing:border-box;width:100px;height:100px}@keyframes
 spinnerCircularAnimate{0%{transform:rotate(0)}to{transform:rotate(360deg)}}html,body{color:#000000de}.spinner
circular__index-page{border-radius:50%;border:10px solid #008787;border-top:10px
 solid transparent;animation:spinnerCircularAnimate .85s ease-in-out infinite}</
style><link rel="stylesheet" href="styles.f17bbdd981b6f3fb.css" media="print"
 onload="this.media='all'"><noscript><link rel="stylesheet" href="styles.f17bbdd981b6f3fb.css"></
noscript></head>
  <body>
    <tp-root>
      <!-- loading layout replaced by app after startupp -->
      <div id="square" class="square">
        <div [...]
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

See Also

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/11, Modification date: 2022/02/23

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following IPv4 addresses are set on the remote host :

 - 172.31.8.1 (on interface br-db93bafdc65d)
 - 172.17.0.1 (on interface docker0)
 - 172.16.2.216 (on interface eth0)
 - 192.168.4.127 (on interface eth1)
 - 127.0.0.1 (on interface lo)
 - 192.168.5.1 (on interface wlan0)
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/16, Modification date: 2019/03/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

118956 - nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its Server response header, the installed version of nginx is 1.x prior to 1.14.1 or 1.15.x prior to 1.15.6. It is, therefore, affected by the following issues :
- An unspecified error exists related to the module 'ngx_http_v2_module' that allows excessive memory usage. (CVE-2018-16843)
- An unspecified error exists related to the module 'ngx_http_v2_module' that allows excessive CPU usage. (CVE-2018-16844)
- An unspecified error exists related to the module 'ngx_http_mp4_module' that allows worker process crashes or memory disclosure. (CVE-2018-16845)

See Also

http://mailman.nginx.org/pipermail/nginx-announce/2018/000220.html

http://mailman.nginx.org/pipermail/nginx-announce/2018/000221.html

http://nginx.org/en/security_advisories.html

Solution

Upgrade to nginx 1.14.1 / 1.15.6 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.0

CVSS v3.0 Base Score

6.1 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H)

CVSS v3.0 Temporal Score

5.3 (E:U/RL:O/RC:C)

CVSS Base Score

5.8 (AV:N/AC:M/Au:N/C:P/I:N/A:P)

CVSS Temporal Score

4.3 (E:U/RL:OF/RC:C)

References

CVE	CVE-2018-16844
CVE	CVE-2018-16845
CVE	CVE-2018-16843
BID	105868

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2018/11/14, Modification date: 2022/04/11

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Installed version : 1.10.3
Fixed version     : 1.14.1
```

141394 - Apache HTTP Server Installed (Linux)

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/10/12, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Path               : /usr/sbin/apache2
Version            : 2.4.25
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS      : True
Running            : no

Configs found :
  - /etc/apache2/apache2.conf

Loaded modules :
  - mod_access_compat
  - mod_alias
  - mod_auth_basic
  - mod_authn_core
  - mod_authn_file
  - mod_authz_core
  - mod_authz_host
  - mod_authz_user
  - mod_autoindex
  - mod_deflate
  - mod_dir
  - mod_env
  - mod_filter
  - mod_mime
  - mod_mpm_event
  - mod_negotiation
  - mod_reqtimeout
  - mod_setenvif
  - mod_status
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

See Also

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/12/21, Modification date: 2023/02/07

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Nessus has enumerated the path of the current scan user :

/usr/local/bin
/usr/bin
/bin
/usr/games
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/11/27, Modification date: 2020/08/20

Ports

security-aig-301.itest.conn.com (UDP/0) Vulnerability State: Resurfaced

```
For your information, here is the traceroute from 192.168.0.160 to 172.16.2.216 :
192.168.0.160
172.16.2.216

Hop Count: 1
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2000/04/28, Modification date: 2022/06/17

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The following title tag will be used :
ThingsPro® Edge
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

See Also

Solution

Disable any unused interfaces.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/06/30, Modification date: 2022/12/20

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following MAC addresses exist on the remote host :

  - 00:90:e8:8f:ef:7d (interface eth1)
  - 5a:65:5d:a6:ca:78 (interface vethc7e1984)
  - 02:42:ea:77:6e:92 (interface br-db93bafdc65d)
  - 9e:21:95:88:b2:90 (interface wwan0)
  - d6:d7:5f:82:be:70 (interface veth8b0dfc3)
  - 00:0e:8e:9c:8b:b2 (interface wlan0)
  - 02:42:95:39:d5:4d (interface docker0)
  - 96:70:42:07:94:71 (interface vethbe34269)
  - c2:38:01:85:83:7f (interface vethc22aed9)
  - ca:50:4d:3b:e0:33 (interface vethb3c47cf)
  - 00:90:e8:8f:ef:7c (interface eth0)
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/01, Modification date: 2021/02/03

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
This port supports TLSv1.2.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.
Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

See Also

Solution

Install the patches listed below.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/07/08, Modification date: 2023/02/08

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
. You need to take the following action :

[ nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE (150154) ]

+ Action to take : Upgrade to nginx 1.20.1 or later.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).
```

127907 - nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple denial of service vulnerabilities.

Description

According to its Server response header, the installed version of nginx is 1.9.5 prior to 1.16.1 or 1.17.x prior to 1.17.3. It is, therefore, affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional conditions. An unauthenticated, remote attacker can exploit this, by manipulating the window size and stream priority of a large data request, to cause a denial of service condition. (CVE-2019-9511)
- A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional conditions. An unauthenticated, remote attacker can exploit this, by creating multiple request streams and continually shuffling the priority of the streams, to cause a denial of service condition. (CVE-2019-9513)
- A denial of service vulnerability exists in the HTTP/2 protocol stack due to improper handling of exceptional conditions. An unauthenticated, remote attacker can exploit this, by sending a stream of headers with a zero length header name and zero length header value, to cause a denial of service condition. (CVE-2019-9516)

See Also

http://www.nessus.org/u?b562be58

http://www.nessus.org/u?5ca4073f

http://www.nessus.org/u?98fc786c

Solution

Upgrade to nginx version 1.16.1 / 1.17.3 or later.

Risk Factor

High

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (E:U/RL:O/RC:C)

CVSS Base Score

7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS Temporal Score

5.8 (E:U/RL:OF/RC:C)

References

CVE	CVE-2019-9516
CVE	CVE-2019-9511
CVE	CVE-2019-9513

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2019/08/16, Modification date: 2022/12/05

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Installed version : 1.10.3
Fixed version     : 1.16.1 / 1.17.3
```

134220 - nginx < 1.17.7 Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

2.2

CVSS v3.0 Base Score

5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (E:U/RL:O/RC:C)

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.2 (E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2019-20372
XREF	IAVB:2020-B-0013-S

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2020/03/05, Modification date: 2022/04/11

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Installed version : 1.10.3
Fixed version     : 1.17.7
```

136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

https://www.nginx.com

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/05/05, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Version           : 1.10.3
Detection Method : Binary Located via Search
Full Version      : 1.10.3
Nginx Plus        : False
```

150154 - nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE

Synopsis

The remote web server is affected by a remote code execution vulnerability.

Description

According to its Server response header, the installed version of nginx is 0.6.18 prior to 1.20.1. It is, therefore, affected by a remote code execution vulnerability. A security issue in nginx resolver was identified, which might allow an unauthenticated remote attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html

http://nginx.org/download/patch.2021.resolver.txt

Solution

Upgrade to nginx 1.20.1 or later.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.0

CVSS v3.0 Base Score

7.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L)

CVSS v3.0 Temporal Score

6.9 (E:P/RL:O/RC:C)

CVSS Base Score

6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.3 (E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-23017
XREF	IAVB:2021-B-0031
XREF	CWE:193

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/06/03, Modification date: 2022/09/15

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Path              : /boot_device/p2/lower/usr/sbin/nginx
Installed version : 1.10.3
Fixed version     : 1.20.1 / 1.21.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.
Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.
Note that this plugin only checks for the options of the remote SSH server.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/09/23, Modification date: 2022/04/05

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Active

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

166602 - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/10/27, Modification date: 2022/10/27

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The FQDN for the remote host has been determined to be:

  FQDN       : security-aig-301.itest.conn.com
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```

170170 - Enumerate the Network Interaface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2023/01/19, Modification date: 2023/01/19

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
vethb3c47cf:
  IPv6:
    - Address : fe80::c850:4dff:fe3b:e033
        Prefixlen : 64
vethc22aed9:
  IPv6:
    - Address : fe80::c038:1ff:fe85:837f
        Prefixlen : 64
vethbe34269:
  IPv6:
    - Address : fe80::9470:42ff:fe07:9471
        Prefixlen : 64
br-db93bafdc65d:
  IPv4:
    - Address : 172.31.8.1
        Netmask : 255.255.252.0
        Broadcast : 172.31.11.255
  IPv6:
    - Address : fe80::42:eaff:fe77:6e92
        Prefixlen : 64
wlan0:
  IPv4:
    - Address : 192.168.5.1
        Netmask : 255.255.255.0
        Broadcast : 192.168.5.255
wwan0:
vethc7e1984:
  IPv6:
    - Address : fe80::5865:5dff:fea6:ca78
        Prefixlen : 64
veth8b0dfc3:
  IPv6:
    - Address : fe80::d4d7:5fff:fe82:be70
        Prefixlen : 64
can0:
eth1:
  IPv4:
    - Address : 192.168.4.127
```

```
        Netmask : 255.255.255.0
        Broadcast : 192.168.4.255
eth0:
  IPv4:
    - Address : 172.16.2.216
        Netmask : 255.255.248.0
        Broadcast : 172.16.7.255
  IPv6:
    - Address : fe80::290:e8ff:fe8f:ef7c
        Prefixlen : 64
docker0:
  IPv4:
    - Address : 172.17.0.1
        Netmask : 255.255.0.0
        Broadcast : 172.17.255.255
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2020/09/22

Ports

security-aig-301.itest.conn.com (TCP/22) Vulnerability State: Resurfaced

```
SSH version : SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
SSH supported authentication : publickey,password
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
 Subject Name:

State/Province: Taiwan
Locality: New Taipei City
Organization: Moxa Inc.
Common Name: ThingsPro Edge Gateway Certificate for HTTPS

Issuer Name:

State/Province: Taiwan
Locality: New Taipei City
Organization: Moxa Inc.
Common Name: ThingsPro Edge Root CA for HTTPS

Serial Number: 00 C6 EE 2A 50 D2 18 5F 63 F5 6B 39 B4 3E 61 F3 4E

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 12 01:58:28 2023 GMT
Not Valid After: May 16 01:58:28 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E3 67 80 C6 C1 58 28 DC CF 49 9B 5F B8 08 B1 AE 91 B8 8B
            C2 DE 0D 7F 55 C3 DB 02 7E 99 A8 BE 20 29 6A 99 E7 DA 0E 84
            6A B5 21 75 85 09 5D 3C 68 60 C3 7D 59 C2 E6 A3 4D A9 1D BA
            52 E6 33 AE 85 4D 14 10 44 06 F5 5B 05 8B 2F FC EC 35 0A 2C
            8F 53 4D 40 CD C2 9F 3B 39 CA 16 56 99 2D 19 91 CF F3 57 2B
            41 E3 18 1F 2B 04 3E FA 54 EB 23 FA 6A F0 5C 34 C3 90 37 04
            F5 53 86 2B 63 93 EA B7 9E C7 F0 B1 9C 24 05 35 4D C0 40 56
            E3 24 05 B8 0C 34 06 B6 2F 25 32 A1 CE 1A E0 E1 C7 DD FF 06
            10 1D BA 95 9D 1A 59 26 A1 90 05 6F 3A DD 43 64 8A 56 57 EB
            D8 1F 56 01 81 FF 6B C3 2D 6C 7F 96 AA CF D4 D3 84 9F FD 34
            3C F8 CD 44 6E 54 DA 0D AC 7D 56 70 7B 36 21 08 D8 D0 67 7F
            18 E5 B8 74 A9 76 2C E3 C8 A0 46 43 A7 21 66 B6 7B 59 21 CE
            40 77 DC 1C F7 85 C1 00 B4 9F DE 3C FF CD 66 72 B3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 6B 2B 37 53 CF 1B 64 5F 0E 22 37 23 A5 A9 DC B1 16 36 22
           BE B1 AE BA 00 3E B2 EA 36 2F 4D 9C D4 5D 4B C9 00 CB 20 FC
           3A 25 90 DA 63 5E 7A 5A 55 14 1C D2 87 A3 49 03 EB EA EA 70
           E2 F8 34 04 B6 06 49 18 76 8D 8B 5F 78 EE 94 62 5F E3 A6 C1
           22 21 EA 5D FB 5C 81 19 2B 6F A3 8B 3D F0 9B 77 82 C8 C8 2E
           A6 CB D7 CA 3E E3 59 11 98 1E B3 9F 33 E9 6A CE FE FA C0 74
           89 27 61 9F 09 82 99 47 74 51 99 74 [...]
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/19, Modification date: 2020/05/13

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
The following card manufacturers were identified :

00:90:E8:8F:EF:7D : MOXA TECHNOLOGIES CORP., LTD.
00:0E:8E:9C:8B:B2 : SparkLAN Communications, Inc.
00:90:E8:8F:EF:7C : MOXA TECHNOLOGIES CORP., LTD.
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX          Auth     Encryption
MAC
   ----------------------        ----------       ---          ----     ---------------------
---
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH         RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH         RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
```

```
   AES128-SHA                  0x00, 0x2F      RSA          RSA      AES-CBC(128)
SHA1
   AES256-SHA                  0x00, 0x35      RSA          RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA             0x00, 0x41      RSA          RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA             0x00, 0x84      RSA          RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA256     0xC0, 0x27      ECDH         RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384     0xC0, 0x28      ECDH         RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256           0x00, 0x3C      RSA          RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256           0x00, 0x3D      RSA          RSA      AES-CBC(256)
SHA256
   RSA-CAMELLIA128-SHA256      0x00, 0xBA      RSA          RSA      Camellia-CBC(128)
SHA256
   RSA-CAMELLIA256-SHA256      0x00, 0xC0      RSA          RSA      Camellia-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

84239 - Debugging Log Report

Synopsis

This plugin gathers the logs written by other plugins and reports them.

Description

Logs generated by other plugins are reported by this plugin. Plugin debugging must be enabled in the policy in order for this plugin to run.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/06/17, Modification date: 2022/04/25

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Plugin debug log(s) have been attached.
```

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/12/08, Modification date: 2021/02/03

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
NPN Supported Protocols:

  http/1.1
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Resurfaced

```
The following sitemap was created from crawling linkable content on the target host :

  - https://security-aig-301.itest.conn.com:8443/
  - https://security-aig-301.itest.conn.com:8443/favicon.ico
  - https://security-aig-301.itest.conn.com:8443/styles.f17bbdd981b6f3fb.css

Attached is a copy of the sitemap file.
```

112154 - Nessus Launched Plugin List

Synopsis

This plugin displays information about the launched plugins.

Description

This plugin displays the list of launched plugins in a semicolon delimited list.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/08/28, Modification date: 2018/09/24

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
[...]
```

156000 - Apache Log4j Installed (Linux / Unix)

Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.
The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.
Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://logging.apache.org/log4j/2.x/

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0941
XREF	IAVA:0001-A-0650

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/12/10, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Resurfaced

```
Nessus detected 2 installs of Apache Log4j:

  Path                           : /boot_device/p2/lower/usr/share/java/libintl.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection

  Path                           : /usr/share/java/libintl.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection


Note: Jar file inspection cannot be performed.  No results or cannot list archive contents.  If
 results are present, install an unzip package to resolve this problem.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
TLSv1.3:
- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256
TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384
This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/01/20, Modification date: 2022/04/06

Ports

security-aig-301.itest.conn.com (TCP/8443) Vulnerability State: Active

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites
outlined below:


 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX          Auth     Encryption
MAC
   ----------------------        ----------       ---          ----     --------------------
---
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH         RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH         RSA      Camellia-CBC(256)
SHA384
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA          RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA          RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA          RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA          RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA          RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
```

```
   AES128-SHA                  0x00, 0x2F      RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                  0x00, 0x35      RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA             0x00, 0x41      RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA             0x00, 0x84      RSA           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA256     0xC0, 0x27      ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384     0xC0, 0x28      ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256           0x00, 0x3C      [...]
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

See Also

https://openssl.org/

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/11/21, Modification date: 2023/02/06

Ports

security-aig-301.itest.conn.com (TCP/0) Vulnerability State: Active

```
  Path    : openssl (via package manager)
  Version : 1.1.0l

We are unable to retrieve version info from the following list of OpenSSL files. However, they may
 include their OpenSSL version in full or part at the end of their names.

e.g. libssl.so.3 (OpenSSl 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/arm-linux-gnueabihf/libcrypto.so.1.0.2
/usr/lib/arm-linux-gnueabihf/libcrypto.so.1.1
/usr/lib/arm-linux-gnueabihf/libssl.so.1.0.2
/usr/lib/arm-linux-gnueabihf/libssl.so.1.1
```

Assets Summary (Executive)

security-aig-301.itest.conn.com

Summary

Critical	High	Medium	Low	Info	Total
1	3	3	0	63	70

Details

Severity	Plugin Id	Name
Critical	33850	Unix Operating System Unsupported Version Detection
High	150154	nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE
High	127907	nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilities
High	118151	nginx Data Disclosure Vulnerability
Medium	118956	nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilities
Medium	51192	SSL Certificate Cannot Be Trusted
Medium	134220	nginx < 1.17.7 Information Disclosure
Info	149334	SSH Password Authentication Accepted
Info	45590	Common Platform Enumeration (CPE)
Info	87242	TLS NPN Supported Protocol Enumeration
Info	45405	Reachable IPv6 address
Info	70657	SSH Algorithms and Languages Supported
Info	142640	Apache HTTP Server Site Enumeration
Info	170170	Enumerate the Network Interaface configuration via SSH
Info	25202	Enumerate IPv6 Interfaces via SSH
Info	84502	HSTS Missing From HTTPS Server
Info	100158	SSH Combined Host Command Logging (Plugin Debugging)
Info	141394	Apache HTTP Server Installed (Linux)
Info	168007	OpenSSL Installed (Linux)
Info	56468	Time of Last System Startup
Info	136318	TLS Version 1.2 Protocol Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	55472	Device Hostname
Info	22964	Service Detection
Info	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
Info	110483	Unix / Linux Running Processes Information

Info	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)
Info	21643	SSL Cipher Suites Supported
Info	22869	Software Enumeration (SSH)
Info	10863	SSL Certificate Information
Info	95928	Linux User List Enumeration
Info	112154	Nessus Launched Plugin List
Info	34277	Nessus UDP Scanner
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	66334	Patch Report
Info	136340	nginx Installed (Linux/UNIX)
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	110385	Target Credential Issues by Authentication Protocol - Insufficient Privilege
Info	10881	SSH Protocol Versions Supported
Info	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
Info	156899	SSL/TLS Recommended Cipher Suites
Info	56984	SSL / TLS Versions Supported
Info	54615	Device Type
Info	117887	OS Security Patch Assessment Available
Info	25220	TCP/IP Timestamps Supported
Info	168980	Enumerate the PATH Variables
Info	33276	Enumerate MAC Addresses via SSH
Info	84821	TLS ALPN Supported Protocol Enumeration
Info	11936	OS Identification
Info	10386	Web Server No 404 Error Code Check
Info	10287	Traceroute Information
Info	25203	Enumerate IPv4 Interfaces via SSH
Info	10335	Nessus TCP scanner
Info	84239	Debugging Log Report
Info	86420	Ethernet MAC Addresses

Info	10267	SSH Server Type and Version Information
Info	157358	Linux Mounted Devices
Info	156000	Apache Log4j Installed (Linux / Unix)
Info	19506	Nessus Scan Information
Info	62564	TLS Next Protocols Supported
Info	91815	Web Application Sitemap
Info	151883	Libgcrypt Installed (Linux/UNIX)
Info	153588	SSH SHA-1 HMAC Algorithms Enabled
Info	152743	Unix Software Discovery Commands Not Available
Info	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
Info	102094	SSH Commands Require Privilege Escalation
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	90707	SSH SCP Protocol Detection

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 88% of the vulnerabilities on the network:

Action to take	Vulns	Assets
nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE: Upgrade to nginx 1.20.1 or later.	8	1

Audits FAILED

1.1.1.1 Ensure mounting of freevxfs filesystems is disabled - modprobe

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/freevxfs.conf and add the following line:
install freevxfs /bin/true
Run the following command to unload the freevxfs module:
rmmod freevxfs

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print
 "fail"}'' returned :

modprobe: FATAL: Module freevxfs not found in directory /lib/modules/4.4.0-cip-rt-moxa-imx7d-
aig-301
fail
```

1.1.1.2 Ensure mounting of jffs2 filesystems is disabled - modprobe

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/jffs2.conf and add the following line:
install jffs2 /bin/true
Run the following command to unload the jffs2 module:
rmmod jffs2

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'' returned :

fail
```

1.1.1.3 Ensure mounting of hfs filesystems is disabled - modprobe

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line:
install hfs /bin/true
Run the following command to unload the hfs module:
rmmod hfs

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v hfs | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}''
 returned :

modprobe: FATAL: Module hfs not found in directory /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301
fail
```

1.1.1.4 Ensure mounting of hfsplus filesystems is disabled - modprobe

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfsplus.conf and add the following line:
install hfsplus /bin/true
Run the following command to unload the hfsplus module:
rmmod hfsplus

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v hfsplus  | /usr/bin/awk '{print} END {if (NR == 0) print
 "fail"}'' returned :

modprobe: FATAL: Module hfsplus not found in directory /lib/modules/4.4.0-cip-rt-moxa-imx7d-
aig-301
fail
```

1.1.1.5 Ensure mounting of udf filesystems is disabled - modprobe

Info

The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.
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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line:
install udf /bin/true
Run the following command to unload the udf module:
rmmod udf

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v udf | /usr/bin/awk '{print} END {if (NR == 0) print "fail"}'' 
 returned :

modprobe: FATAL: Module udf not found in directory /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301
fail
```

1.1.10 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

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /var/tmp partition. See the fstab(5) manual page for more information.
Run the following command to remount /var/tmp:
mount -o remount,noexec /var/tmp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-53	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.11 Ensure separate partition exists for /var/log

Info

The /var/log directory is used by system services to store log data.
Rationale:
There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Solution

For new installations, during installation create a custom partition setup and specify a separate partition for /var/log.
For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.
Impact:
Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/log' did not return any result
```

1.1.12 Ensure separate partition exists for /var/log/audit

Info

The auditing daemon, auditd, stores log data in the /var/log/audit directory.
Rationale:
There are two important reasons to ensure that data gathered by auditd is stored on a separate partition: protection against resource exhaustion (since the audit.log file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as syslog) consume space in the same partition as auditd, it may not perform as desired.

Solution

For new installations, during installation create a custom partition setup and specify a separate partition for /var/log/audit.
For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.
Impact:
Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV6	3.1
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/log/audit' did not return any result
```

1.1.13 Ensure separate partition exists for /home

Info

The /home directory is used to support disk storage needs of local users.
Rationale:
If the system is intended to support local users, create a separate partition for the /home directory to protect against resource exhaustion and restrict the type of files that can be stored under /home.

Solution

For new installations, during installation create a custom partition setup and specify a separate partition for /home.
For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.
Impact:
Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /home' did not return any result
```

1.1.14 Ensure nodev option set on /home partition

Info

The nodev mount option specifies that the filesystem cannot contain special devices.
Rationale:
Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Solution

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /home partition. See the fstab(5) manual page for more information.
mount -o remount,nodev /home
Notes:
The actions in this recommendation refer to the /home partition, which is the default user partition that is defined in many distributions. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /home' did not return any result
```

1.1.17 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

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information.
Run the following command to remount /dev/shm:
mount -o remount,noexec /dev/shm

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	CM-11
800-53	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV7	2.6
CSCV7	8
CSF	DE.CM-3
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1
ISO/IEC-27001	A.12.6.2

ITSG-33	SI-3
LEVEL	1S
NIAV2	GS8a
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
```

1.1.18 Ensure nodev option set on removable media partitions

Info

The nodev mount option specifies that the filesystem cannot contain special devices.
Rationale:
Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as /dev/kmemor the raw disk partitions.

Solution

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the fstab(5) manual page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.19 Ensure nosuid option set on removable media partitions

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

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the fstab(5) manual page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.2 Ensure /tmp is configured - mount

Info

The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.
Rationale:
Making /tmp its own file system allows an administrator to set 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 hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.
This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Solution

Configure /etc/fstab as appropriate.
example:
tmpfs/tmptmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
OR Run the following commands to enable systemd /tmp mounting:
systemctl unmask tmp.mount systemctl enable tmp.mount
Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount:
[Mount] What=tmpfs Where=/tmp Type=tmpfs Options=mode=1777,strictatime,noexec,nodev,nosuid
Impact:
Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.
Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it 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.
/tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/
https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
Notes:
If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.2 Ensure /tmp is configured - systemctl

Info

The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.
Rationale:
Making /tmp its own file system allows an administrator to set 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 hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.
This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Solution

Configure /etc/fstab as appropriate.
example:
tmpfs/tmptmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
OR Run the following commands to enable systemd /tmp mounting:
systemctl unmask tmp.mount systemctl enable tmp.mount
Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount:
[Mount] What=tmpfs Where=/tmp Type=tmpfs Options=mode=1777,strictatime,noexec,nodev,nosuid
Impact:
Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.
Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it 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.
/tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/
https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
Notes:
If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/systemctl is-enabled tmp.mount' returned :
```

```
Failed to get unit file state for tmp.mount: No such file or directory
```

1.1.20 Ensure noexec option set on removable media partitions

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 the removable media. This deters users from being able to introduce potentially malicious software on the system.

Solution

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the fstab(5) manual page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	CM-11
800-53	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV7	2.6
CSCV7	8
CSF	DE.CM-3
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1
ISO/IEC-27001	A.12.6.2
ITSG-33	SI-3

LEVEL	1NS
NIAV2	GS8a
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep -P 'on[\s]+/dev/(floppy|cdrom|corder|mmcblk)'' did not return
 any result
```

1.1.3 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 attempt to create block or character special devices in /tmp.

Solution

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount:
[Mount] What=tmpfs Where=/tmp Type=tmpfs Options=mode=1777,strictatime,noexec,nodev,nosuid
Run the following commands to enable systemd /tmp mounting:
systemctl unmask tmp.mount systemctl enable tmp.mount
Notes:
systemd includes the tmp.mount service which should be used instead of configuring /etc/fstab. Mounting options are configured in the Options setting in /etc/systemd/system/local-fs.target.wants/tmp.mount.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.4 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

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to add nodev to the /tmp mount options:
[Mount] Options=mode=1777,strictatime,noexec,nodev,nosuid
Run the following command to remount /tmp :
mount -o remount,nodev /tmp
Notes:
systemd includes the tmp.mount service which should be used instead of configuring /etc/fstab. Mounting options are configured in the Options setting in /etc/systemd/system/local-fs.target.wants/tmp.mount.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.5 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 .

Solution

Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to add noexec to the /tmp mount options:
[Mount] Options=mode=1777,strictatime,noexec,nodev,nosuid
Run the following command to remount /tmp :
mount -o remount,noexec /tmp
Notes:
systemd includes the tmp.mount service which should be used instead of configuring /etc/fstab. Mounting options are configured in the Options setting in /etc/systemd/system/local-fs.target.wants/tmp.mount.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	CM-11
800-53	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV7	2.6
CSCV7	8
CSF	DE.CM-3
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1

ISO/IEC-27001	A.12.6.2
ITSG-33	SI-3
LEVEL	1S
NIAV2	GS8a
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /tmp' did not return any result
```

1.1.6 Ensure separate partition exists for /var

Info

The /var directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.
Rationale:
Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Solution

For new installations, during installation create a custom partition setup and specify a separate partition for /var.
For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.
Impact:
Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.
References:
AJ Lewis, 'LVM HOWTO', http://tldp.org/HOWTO/LVM-HOWTO/

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var' did not return any result
```

1.1.7 Ensure separate partition exists for /var/tmp

Info

The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications.
Rationale:
Since the /var/tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making /var/tmp its own file system allows an administrator to set the noexec option on the mount, making /var/tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink 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.

Solution

For new installations, during installation create a custom partition setup and specify a separate partition for /var/tmp .
For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.
Impact:
Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.8 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 attempt to create block or character special devices in /var/tmp.

Solution

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/tmp partition. See the fstab(5) manual page for more information.
Run the following command to remount /var/tmp:
mount -o remount,nodev /var/tmp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.1.9 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

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/tmp partition. See the fstab(5) manual page for more information.
Run the following command to remount /var/tmp:
mount -o remount,nosuid /var/tmp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /var/tmp' did not return any result
```

1.3.1 Ensure AIDE is installed

Info

AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.
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:
apt-get install aide aide-common
Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.
Initialize AIDE:
aideinit
References:
AIDE stable manual: http://aide.sourceforge.net/stable/manual.html
Notes:
The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run prelink -ua to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	2.2
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s aide 2>&1' returned :

dpkg-query: package 'aide' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

1.3.2 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

Run the following command:
crontab -u root -e
Add the following line to the crontab:
0 5 * * * /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check
Notes:
The checking in this recommendation occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.
Note that Debian advises using /usr/bin/aide.wrapper rather than calling /usr/bin/aide directly in order to protect the database and prevent conflicts.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e

NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

1.4.1 Ensure permissions on bootloader config are configured

Info

The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually grub.cfg stored in /boot/grub.
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 commands to set permissions on your grub configuration:
chown root:root /boot/grub/grub.cfg # chmod og-rwx /boot/grub/grub.cfg
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.4.2 Ensure bootloader password is set - password_pbkdf2

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).

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:
grub-mkpasswd-pbkdf2 Enter password: <password>
Reenter password: <password>
Your PBKDF2 is <encrypted-password>
Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file:
cat <<EOF set superusers='<username>'
password_pbkdf2 <username> <encrypted-password>
EOF
If there is a requirement to be able to boot/reboot without entering the password, edit /etc/grub.d/10_linux and add --unrestricted to the line CLASS= Example:
CLASS='--class gnu-linux --class gnu --class os --unrestricted'
Run the following command to update the grub2 configuration:
update-grub
Impact:
If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing 'e' or access the GRUB 2 command line by pressing 'c'
If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem
You can add --unrestricted to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.
More Information: https://help.ubuntu.com/community/Grub2/Passwords
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.4.2 Ensure bootloader password is set - set superusers

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).

Solution

Create an encrypted password with grub-mkpasswd-pbkdf2:
grub-mkpasswd-pbkdf2 Enter password: <password>
Reenter password: <password>
Your PBKDF2 is <encrypted-password>
Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file:
cat <<EOF set superusers='<username>'
password_pbkdf2 <username> <encrypted-password>
EOF
If there is a requirement to be able to boot/reboot without entering the password, edit /etc/grub.d/10_linux and add --unrestricted to the line CLASS= Example:
CLASS='--class gnu-linux --class gnu --class os --unrestricted'
Run the following command to update the grub2 configuration:
update-grub
Impact:
If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing 'e' or access the GRUB 2 command line by pressing 'c'
If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem
You can add --unrestricted to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.
More Information: https://help.ubuntu.com/community/Grub2/Passwords
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.5.1 Ensure core dumps are restricted - limits.conf limits.d

Info

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

Solution

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file:
* hard core 0
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
fs.suid_dumpable = 0
Run the following command to set the active kernel parameter:
sysctl -w fs.suid_dumpable=0

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*
\*[[:space:]]+hard[[:space:]]+core[[:space:]]+0[[:space:]]*$' /etc/security/limits.conf /etc/
security/limits.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}''
 returned :

fail
```

1.5.2 Ensure XD/NX support is enabled

Info

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.
Rationale:
Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Solution

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems:
If necessary configure your bootloader to load the new kernel and reboot the system.
You may need to enable NX or XD support in your bios.
Notes:
Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	SC-39
800-53	SI-16
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1NS
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/dmesg | /bin/grep 'NX (Execute' 2>&1' did not return any result
```

1.5.3 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 /etc/sysctl.d/* file:
kernel.randomize_va_space = 2
Run the following command to set the active kernel parameter:
sysctl -w kernel.randomize_va_space=2

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	SC-39
800-53	SI-16
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1S
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -P '^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*$' /etc/
sysctl.conf /etc/sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print
 "fail"}'' returned :

fail
```

1.6.1.1 Ensure SELinux is enabled in the bootloader configuration - security=selinux

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.

Solution

run the following command to configure GRUB and PAM and to create /.autorelabel
selinux-activate
Edit /etc/default/grub and add the following parameters to the GRUB_CMDLINE_LINUX= line:
selinux=1 security=selinux
example:
GRUB_CMDLINE_LINUX_DEFAULT='quiet'
GRUB_CMDLINE_LINUX='selinux=1 security=selinux enforcing=1 audit=1'
Run the following command to update the grub2 configuration:
update-grub
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1

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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.6.1.1 Ensure SELinux is enabled in the bootloader configuration - selinux = 1

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.

Solution

run the following command to configure GRUB and PAM and to create /.autorelabel
selinux-activate
Edit /etc/default/grub and add the following parameters to the GRUB_CMDLINE_LINUX= line:
selinux=1 security=selinux
example:
GRUB_CMDLINE_LINUX_DEFAULT='quiet'
GRUB_CMDLINE_LINUX='selinux=1 security=selinux enforcing=1 audit=1'
Run the following command to update the grub2 configuration:
update-grub
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1

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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.6.1.2 Ensure the SELinux state is enforcing - /etc/selinux/config

Info

Set SELinux to enable when the system is booted.
Rationale:
SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.

Solution

Edit the /etc/selinux/config file to set the SELINUX parameter:
SELINUX=enforcing
Edit /etc/default/grub and add the following parameters to the GRUB_CMDLINE_LINUX= line:
enforcing=1
Example:
GRUB_CMDLINE_LINUX_DEFAULT='quiet'
GRUB_CMDLINE_LINUX='selinux=1 security=selinux enforcing=1 audit=1'
Run the following command to update the grub2 configuration:
update-grub

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/selinux/config
```

1.6.1.2 Ensure the SELinux state is enforcing - sestatus

Info

Set SELinux to enable when the system is booted.
Rationale:
SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.

Solution

Edit the /etc/selinux/config file to set the SELINUX parameter:
SELINUX=enforcing
Edit /etc/default/grub and add the following parameters to the GRUB_CMDLINE_LINUX= line:
enforcing=1
Example:
GRUB_CMDLINE_LINUX_DEFAULT='quiet'
GRUB_CMDLINE_LINUX='selinux=1 security=selinux enforcing=1 audit=1'
Run the following command to update the grub2 configuration:
update-grub

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sestatus' returned :

bash: /usr/sbin/sestatus: No such file or directory
```

1.6.1.3 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=default
Notes:
If your organization requires stricter policies, ensure that they are set in the /etc/selinux/config file.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/selinux/config
```

1.6.2.1 Ensure AppArmor is enabled in the bootloader configuration - apparmor=1

Info

Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters.
Rationale:
AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

Solution

edit /etc/default/grub and add the appermor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line
GRUB_CMDLINE_LINUX='apparmor=1 security=apparmor'
update the grub configuration
update-grub
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.6.2.1 Ensure AppArmor is enabled in the bootloader configuration - security=apparmor

Info

Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters.
Rationale:
AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

Solution

edit /etc/default/grub and add the appermor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line
GRUB_CMDLINE_LINUX='apparmor=1 security=apparmor'
update the grub configuration
update-grub
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /boot/grub/grub.cfg
```

1.6.2.2 Ensure all AppArmor Profiles are enforcing - 0 processes are unconfined

Info

AppArmor profiles define what resources applications are able to access.
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 any policies that exist on the system are activated.

Solution

Run the following command to set all profiles to enforce mode:
aa-enforce /etc/apparmor.d/*
Any unconfined processes may need to have a profile created or activated for them and then be restarted.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/apparmor_status' returned :

bash: /usr/sbin/apparmor_status: No such file or directory
```

1.6.2.2 Ensure all AppArmor Profiles are enforcing - complain mode

Info

AppArmor profiles define what resources applications are able to access.
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 any policies that exist on the system are activated.

Solution

Run the following command to set all profiles to enforce mode:
aa-enforce /etc/apparmor.d/*
Any unconfined processes may need to have a profile created or activated for them and then be restarted.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/apparmor_status' returned :

bash: /usr/sbin/apparmor_status: No such file or directory
```

1.6.2.2 Ensure all AppArmor Profiles are enforcing - profiles loaded

Info

AppArmor profiles define what resources applications are able to access.
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 any policies that exist on the system are activated.

Solution

Run the following command to set all profiles to enforce mode:
aa-enforce /etc/apparmor.d/*
Any unconfined processes may need to have a profile created or activated for them and then be restarted.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/apparmor_status' returned :

bash: /usr/sbin/apparmor_status: No such file or directory
```

1.6.3 Ensure SELinux or AppArmor are installed

Info

SELinux and AppArmor provide Mandatory Access Controls.
Rationale:
Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Solution

Run one of the following commands to install SELinux or apparmor:
apt-get install selinux-basics selinux-policy-default # apt-get install apparmor apparmor-utils

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

1.7.1.2 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
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 , or v , or references to the OS platform
echo 'Authorized uses only. All activity may be monitored and reported.' > /etc/issue

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/issue - regex '(\\[mrsv]|[Dd]ebian)' found - expect '(\\[mrsv]|[Dd]ebian)' found in the
 following lines:
         1: Debian GNU/Linux 9 \n \l
```

1.7.1.3 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 , or v :
echo 'Authorized uses only. All activity may be monitored and reported.' > /etc/issue.net

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/issue.net - regex '(\\[mrsv]|[Dd]ebian)' found - expect '(\\[mrsv]|[Dd]ebian)' found in
 the following lines:
          1: Debian GNU/Linux 9
```

2.2.1.2 Ensure ntp is configured - ntp server

Info

ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.
This recommendation only applies if ntp is in use on the system.
Rationale:
If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:
restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery
Add or edit server or pool lines to /etc/ntp.conf as appropriate:
server <remote-server>
Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:
RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV6	6.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ntp.conf" does not contain "^[\s]*server[\s]+pool.ntp.org[\s]*$"
```

2.2.1.2 Ensure ntp is configured - restrict -4

Info

ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.
This recommendation only applies if ntp is in use on the system.
Rationale:
If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:
restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery
Add or edit server or pool lines to /etc/ntp.conf as appropriate:
server <remote-server>
Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:
RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/ntp.conf - regex '^[\s]*restrict[\s]+-4[\s][^:]' found - expect
 '^[\s]*restrict[\s]+-4[\s]+(,?default[\s]*|,?kod[\s]*|,?nomodify[\s]*|,?notrap[\s]*|,?
nopeer[\s]*|,?noquery[\s]*){6}$' not found in the following lines:
          35: restrict -4 default kod notrap nomodify nopeer noquery limited
```

2.2.1.2 Ensure ntp is configured - restrict -6

Info

ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.
This recommendation only applies if ntp is in use on the system.
Rationale:
If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:
restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery
Add or edit server or pool lines to /etc/ntp.conf as appropriate:
server <remote-server>
Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:
RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/ntp.conf - regex '^[\s]*restrict[\s]+-6[\s][^:]' found - expect
 '^[\s]*restrict[\s]+-6[\s]+(,?default[\s]*|,?kod[\s]*|,?nomodify[\s]*|,?notrap[\s]*|,?
nopeer[\s]*|,?noquery[\s]*){6}$' not found in the following lines:
          36: restrict -6 default kod notrap nomodify nopeer noquery limited
```

2.2.16 Ensure rsync service is not enabled

Info

The rsyncd service can be used to synchronize files between systems over network links.
Rationale:
The rsyncd service presents a security risk as it uses unencrypted protocols for communication.

Solution

Run the following command to disable rsync:
systemctl disable rsync

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1

CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s rsync | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed
```

3.1.1 Ensure IP forwarding is disabled - ipv4 /etc/sysctl.conf /etc/sysctl.d/*

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 the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.ip_forward=0 # sysctl -w net.ipv6.conf.all.forwarding=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.ip_forward[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.1.1 Ensure IP forwarding is disabled - ipv4 sysctl

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 the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.ip_forward=0 # sysctl -w net.ipv6.conf.all.forwarding=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.ip_forward' returned :

net.ipv4.ip_forward = 1
```

3.1.1 Ensure IP forwarding is disabled - ipv6 /etc/sysctl.conf /etc/sysctl.d/*

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 the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.ip_forward=0 # sysctl -w net.ipv6.conf.all.forwarding=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.forwarding[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.1.2 Ensure packet redirect sending is disabled - all /etc/sysctl.conf /etc/sysctl.d/*

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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.1.2 Ensure packet redirect sending is disabled - all sysctl

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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.send_redirects' returned :

net.ipv4.conf.all.send_redirects = 1
```

3.1.2 Ensure packet redirect sending is disabled - default /etc/sysctl.conf /etc/sysctl.d/*

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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.send_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.1.2 Ensure packet redirect sending is disabled - default sysctl

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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.send_redirects' returned :

net.ipv4.conf.default.send_redirects = 1
```

3.2.1 Ensure source routed packets are not accepted - files 'net.ipv4.conf.all.accept_source_route = 0'

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure source routed packets are not accepted - files 'net.ipv4.conf.default.accept_source_route = 0'

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure source routed packets are not accepted - files 'net.ipv6.conf.all.accept_source_route = 0'

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure source routed packets are not accepted - files 'net.ipv6.conf.default.accept_source_route = 0'

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_source_route[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.1 Ensure source routed packets are not accepted - net.ipv4.conf.default.accept_source_route = 0

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.accept_source_route' returned :

net.ipv4.conf.default.accept_source_route = 1
```

3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects'

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.accept_redirects' returned :

net.ipv4.conf.default.accept_redirects = 1
```

3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv6.conf.default.accept_redirects'

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_redirects' returned :

net.ipv6.conf.default.accept_redirects = 1
```

3.2.2 Ensure ICMP redirects are not accepted - files net.ipv4.conf.all.accept_redirects= 0

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.2 Ensure ICMP redirects are not accepted - files net.ipv4.conf.default.accept_redirects= 0

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.2 Ensure ICMP redirects are not accepted - files net.ipv6.conf.all.accept_redirects= 0

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.2 Ensure ICMP redirects are not accepted - files net.ipv6.conf.default.accept_redirects= 0

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.2 Ensure ICMP redirects are not accepted - net.ipv6.conf.all.accept_redirects

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_redirects' returned :

net.ipv6.conf.all.accept_redirects = 1
```

3.2.3 Ensure secure ICMP redirects are not accepted - files net.ipv4.conf.all.secure_redirects = 0

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 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.3 Ensure secure ICMP redirects are not accepted - files net.ipv4.conf.default.secure_redirects = 0

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 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.secure_redirects[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /
usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.3 Ensure secure ICMP redirects are not accepted - net.ipv4.conf.all.secure_redirects = 0

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 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.secure_redirects' returned :

net.ipv4.conf.all.secure_redirects = 1
```

3.2.3 Ensure secure ICMP redirects are not accepted - net.ipv4.conf.default.secure_redirects = 0

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 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.secure_redirects' returned :

net.ipv4.conf.default.secure_redirects = 1
```

3.2.4 Ensure suspicious packets are logged - files net.ipv4.conf.all.log_martians = 1

Info

When enabled, this feature logs packets with un-routable source addresses to the kernel log.
Rationale:
Enabling this feature and 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.4 Ensure suspicious packets are logged - files net.ipv4.conf.default.log_martians = 1

Info

When enabled, this feature logs packets with un-routable source addresses to the kernel log.
Rationale:
Enabling this feature and 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.log_martians[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/
bin/awk '{print} END {if (NR != 0) print "pass"; else print "fail"}'' returned :

fail
```

3.2.4 Ensure suspicious packets are logged - net.ipv4.conf.all.log_martians = 1

Info

When enabled, this feature logs packets with un-routable source addresses to the kernel log.
Rationale:
Enabling this feature and 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.log_martians' returned :

net.ipv4.conf.all.log_martians = 0
```

3.2.4 Ensure suspicious packets are logged - net.ipv4.conf.default.log_martians = 1

Info

When enabled, this feature logs packets with un-routable source addresses to the kernel log.
Rationale:
Enabling this feature and 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 /etc/sysctl.d/* file:
net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.log_martians' returned :

net.ipv4.conf.default.log_martians = 0
```

3.2.5 Ensure broadcast ICMP requests are ignored - files net.ipv4.icmp_echo_ignore_broadcasts = 1

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 parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.icmp_echo_ignore_broadcasts = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.icmp_echo_ignore_broadcasts[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /
etc/sysctl.d/* |/usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}''
 returned :

fail
```

3.2.6 Ensure bogus ICMP responses are ignored - files net.ipv4.icmp_ignore_bogus_error_responses = 1

Info

Setting 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 /etc/sysctl.d/* file:
net.ipv4.icmp_ignore_bogus_error_responses = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.icmp_ignore_bogus_error_responses[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/
sysctl.conf /etc/sysctl.d/* | /usr/bin/awk '{print} END {if (NR != 0) print "pass"; else print
 "fail"}'' returned :

fail
```

3.2.7 Ensure Reverse Path Filtering is enabled - files net.ipv4.conf.all.rp_filter = 1

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 these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.all
\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.7 Ensure Reverse Path Filtering is enabled - files net.ipv4.conf.default.rp_filter = 1

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 these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv4\.conf\.default
\.rp_filter[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* | /usr/bin/
awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.7 Ensure Reverse Path Filtering is enabled - net.ipv4.conf.all.rp_filter = 1

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 these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.rp_filter' returned :

net.ipv4.conf.all.rp_filter = 0
```

3.2.7 Ensure Reverse Path Filtering is enabled - net.ipv4.conf.default.rp_filter = 1

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 these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1
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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.default.rp_filter' returned :

net.ipv4.conf.default.rp_filter = 0
```

3.2.8 Ensure TCP SYN Cookies is enabled - files net.ipv4.tcp_syncookies = 1

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. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.tcp_syncookies = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.tcp_syncookies=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net
\.ipv4\.tcp_syncookies[[:space:]]*=[[:space:]]*1[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/*
 | /usr/bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.9 Ensure IPv6 router advertisements are not accepted - files net.ipv6.conf.all.accept_ra = 0

Info

This setting disables the system's ability to accept IPv6 router advertisements.
Rationale:
It is recommended that systems 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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_ra = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.all
\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.9 Ensure IPv6 router advertisements are not accepted - files net.ipv6.conf.default.accept_ra = 0

Info

This setting disables the system's ability to accept IPv6 router advertisements.
Rationale:
It is recommended that systems 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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_ra = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep -s -E '^[[:space:]]*net\.ipv6\.conf\.default
\.accept_ra[[:space:]]*=[[:space:]]*0[[:space:]]*$' /etc/sysctl.conf /etc/sysctl.d/* |/usr/bin/awk
 '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

3.2.9 Ensure IPv6 router advertisements are not accepted - net.ipv6.conf.all.accept_ra = 0

Info

This setting disables the system's ability to accept IPv6 router advertisements.
Rationale:
It is recommended that systems 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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_ra = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_ra' returned :

net.ipv6.conf.all.accept_ra = 1
```

3.2.9 Ensure IPv6 router advertisements are not accepted - net.ipv6.conf.default.accept_ra = 0

Info

This setting disables the system's ability to accept IPv6 router advertisements.
Rationale:
It is recommended that systems 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.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_ra = 0
Run the following commands 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_ra' returned :

net.ipv6.conf.default.accept_ra = 1
```

3.3.1 Ensure TCP Wrappers is installed

Info

TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. In the past, services that were called from inetd and xinetd supported the use of tcp wrappers. As inetd and xinetd have been falling in disuse, any service that can support tcp wrappers will have the libwrap.so library attached to it.
Rationale:
TCP Wrappers provide a good simple access list mechanism to services that may not have that support built in. It is recommended that all services that can support TCP Wrappers, use it.

Solution

Run the following command to install TCP Wrappers:
apt-get install tcpd
Notes:
To verify if a service supports TCP Wrappers, run the following command:
ldd <path-to-daemon> | grep libwrap.so
If there is any output, then the service supports TCP Wrappers.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV6	9.2
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s tcpd 2>&1' returned :

dpkg-query: package 'tcpd' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

3.3.2 Ensure /etc/hosts.allow is configured

Info

The /etc/hosts.allow file specifies which IP addresses are permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.deny file.
Rationale:
The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.

Solution

Run the following command to create /etc/hosts.allow:
echo 'ALL: <net>/<mask>, <net>/<mask>, ...' >/etc/hosts.allow
where each <net>/<mask> combination (for example, '192.168.1.0/255.255.255.0') represents one network block in use by your organization that requires access to this system.
Notes:
Contents of the /etc/hosts.allow file will vary depending on your network configuration.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/hosts.allow" does not contain "^[\s]*ALL[\s]*:"
```

3.3.3 Ensure /etc/hosts.deny is configured

Info

The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file.
Rationale:
The /etc/hosts.deny file serves as a failsafe so that any host not specified in /etc/hosts.allow is denied access to the system.

Solution

Run the following command to create /etc/hosts.deny:
echo 'ALL: ALL' >> /etc/hosts.deny
Notes:
Contents of the /etc/hosts.deny file may include additional options depending on your network configuration.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/hosts.deny" does not contain "^[\s]*ALL:"
```

3.4.1 Ensure DCCP is disabled - modprobe

Info

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.
Rationale:
If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/dccp.conf and add the following line:
install dccp /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v dccp' returned :

insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/dccp/dccp.ko
```

3.4.2 Ensure SCTP is disabled - modprobe

Info

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/sctp.conf and add the following line:
install sctp /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1

CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v sctp' returned :

insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/lib/libcrc32c.ko
insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/sctp/sctp.ko
```

3.4.3 Ensure RDS is disabled - modprobe

Info

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/rds.conf and add the following line:
install rds /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v rds' returned :

insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/rds/rds.ko
```

3.4.4 Ensure TIPC is disabled - modprobe

Info

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/tipc.conf and add the following line:
install tipc /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/modprobe -n -v tipc' returned :

insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/ipv4/udp_tunnel.ko
insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/ipv6/ip6_udp_tunnel.ko
insmod /lib/modules/4.4.0-cip-rt-moxa-imx7d-aig-301/kernel/net/tipc/tipc.ko
```

3.5.1.1 Ensure default deny firewall policy - Chain FORWARD

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
iptables -P INPUT DROP # iptables -P OUTPUT DROP # iptables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/iptables --list | /bin/grep 'Chain FORWARD'' returned :

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
```

3.5.1.1 Ensure default deny firewall policy - Chain INPUT

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
iptables -P INPUT DROP # iptables -P OUTPUT DROP # iptables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/iptables --list | /bin/grep 'Chain INPUT'' returned :

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)

Perhaps iptables or your kernel needs to be upgraded.
```

3.5.1.1 Ensure default deny firewall policy - Chain OUTPUT

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
iptables -P INPUT DROP # iptables -P OUTPUT DROP # iptables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/iptables --list | /bin/grep 'Chain OUTPUT'' returned :

iptables v1.6.0:
can't initialize iptables table `filter': Permission denied (you must be root)


Perhaps iptables or your kernel needs to be upgraded.
```

3.5.1.2 Ensure loopback traffic is configured - input

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).
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 (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:
iptables -A INPUT -i lo -j ACCEPT # iptables -A OUTPUT -o lo -j ACCEPT # iptables -A INPUT -s 127.0.0.0/8 -j DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
fail
```

3.5.1.2 Ensure loopback traffic is configured - output

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).
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 (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following commands to implement the loopback rules:
iptables -A INPUT -i lo -j ACCEPT # iptables -A OUTPUT -o lo -j ACCEPT # iptables -A INPUT -s 127.0.0.0/8 -j DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
fail
```

3.5.2.1 Ensure IPv6 default deny firewall policy - Chain FORWARD

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain FORWARD'' returned :

ip6tables v1.6.0:
can't initialize ip6tables table `filter': Permission denied (you must be root)


Perhaps ip6tables or your kernel needs to be upgraded.
```

3.5.2.1 Ensure IPv6 default deny firewall policy - Chain INPUT

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain INPUT'' returned :

ip6tables v1.6.0: can't initialize ip6tables table `filter': Permission denied (you must be root)

Perhaps ip6tables or your kernel needs to be upgraded.
```

3.5.2.1 Ensure IPv6 default deny firewall policy - Chain OUTPUT

Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Rationale:
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Solution

Run the following commands to implement a default DROP policy:
ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1

TBA-FIISB 43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/ip6tables --list | /bin/grep 'Chain OUTPUT'' returned :

ip6tables v1.6.0:
can't initialize ip6tables table `filter': Permission denied (you must be root)


Perhaps ip6tables or your kernel needs to be upgraded.
```

3.7 Disable IPv6

Info

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.
Rationale:
If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Solution

Edit /etc/default/grub and add ipv6.disable=1 to the GRUB_CMDLINE_LINUX parameters:
GRUB_CMDLINE_LINUX='ipv6.disable=1'
Run the following command to update the grub2 configuration:
update-grub

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	3.7
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	2NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^[[:space:]]*linux' /boot/grub/grub.cfg' returned :

/bin/grep:
/boot/grub/grub.cfg
: No such file or directory
```

4.1.1.1 Ensure audit log storage size is configured

Info

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.
Rationale:
It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Solution

Set the following parameter in /etc/audit/auditd.conf in accordance with site policy:
max_log_file = <MB>
Notes:
The max_log_file parameter is measured in megabytes.

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV6	6.3
CSCV7	6.4
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	2NS
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/auditd.conf
```

4.1.1.2 Ensure system is disabled when audit logs are full - action_mail_acct

Info

The auditd daemon can be configured to halt the system when the audit logs are full.
Rationale:
In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Solution

Set the following parameters in /etc/audit/auditd.conf:
space_left_action = email action_mail_acct = root admin_space_left_action = halt

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/auditd.conf
```

4.1.1.2 Ensure system is disabled when audit logs are full - admin_space_left_action

Info

The auditd daemon can be configured to halt the system when the audit logs are full.
Rationale:
In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Solution

Set the following parameters in /etc/audit/auditd.conf:
space_left_action = email action_mail_acct = root admin_space_left_action = halt

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/auditd.conf
```

4.1.1.2 Ensure system is disabled when audit logs are full - space_left_action

Info

The auditd daemon can be configured to halt the system when the audit logs are full.
Rationale:
In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Solution

Set the following parameters in /etc/audit/auditd.conf:
space_left_action = email action_mail_acct = root admin_space_left_action = halt

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/auditd.conf
```

4.1.1.3 Ensure audit logs are not automatically deleted

Info

The max_log_file_action setting determines how to handle the audit log file reaching the max file size. A value of keep_logs will rotate the logs but never delete old logs.
Rationale:
In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Solution

Set the following parameter in /etc/audit/auditd.conf:
max_log_file_action = keep_logs

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	2S
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/auditd.conf
```

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl chmod fchmod fchmodat

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep perm_mod' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl chown fchown fchownat lchown

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep perm_mod' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl lsetxattr setxattr fsetxattr removexattr

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep perm_mod' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.10 Ensure discretionary access control permission modification events are collected - chmod fchmod fchmodat

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.10 Ensure discretionary access control permission modification events are collected - chown fchown fchownat lchown

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.10 Ensure discretionary access control permission modification events are collected - lsetxattr setxattr fsetxattr removexattr

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EACCES

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EPERM

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EACCES

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep access' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EPERM

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep access' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.12 Ensure use of privileged commands is collected

Info

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.
Rationale:
Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Solution

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows: -F path=' $1 ' - will populate each file name found through the find command and processed by awk. -F perm=x - will write an audit record if the file is executed. -F auid>=1000 - will write a record if the user executing the command is not a privileged user. -F auid!= 4294967295 - will ignore Daemon events All audit records should be tagged with the identifier 'privileged'.
Run the following command replacing with a list of partitions where programs can be executed from on your system:
find <partition> -xdev (-perm -4000 -o -perm -2000) -type f | awk '{print '-a always,exit -F path=' $1 ' -F perm=x -F auid>=1000 -F auid!=4294967295
-k privileged' }'
Add all resulting lines to the /etc/audit/audit.rules file.
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-12
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-12
LEVEL	2S
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

SWIFT-CSCV1 6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
 The command '(/usr/bin/find / -xdev \( -perm -4000 -o -perm -2000 \) -type f && cat /etc/audit/
audit.rules) | /usr/bin/awk '/^\// { a[$1] = 1 } /^-a .*perm=x/ { p=$0; gsub(/^.*path=/, "", p);
 gsub(/ .*$/, "", p); a[p] = 0 } END { for (p in a) { if (a[p] == 1) { print p; f++ } }; if (!f)
 print "none" }'' returned :

/usr/bin/find: '/etc/chatscripts': Permission denied

/usr/bin/find: '/etc/ppp/peers': Permission denied

/usr/bin/find:
'/etc/ssl/private'
: Permission denied


/usr/bin/find:
'/etc/aziot/edged/config.d'
: Permission denied


/usr/bin/find: '/opt/containerd': Permission denied

/usr/bin/find: '/root': Permission denied

/usr/bin/find: '/var/bruno/apps/opcuaserver/data/certs/mxopcserver/certificationstores/issuer':
 Permission denied

/usr/bin/find: '/var/cache/apt/archives/partial': Permission denied

/usr/bin/find: '/var/cache/ldconfig': Permission denied

/usr/bin/find: '/var/lib/nginx/body': Permission denied

/usr/bin/find: '/var/lib/nginx/fastcgi': Permission denied
/usr/bin/find: '/var/lib/nginx/proxy': Permission denied
/usr/bin/find: '/var/lib/nginx/scgi': Permission denied
/usr/bin/find: '/var/lib/nginx/uwsgi': Permission denied

/usr/bin/find: '/var/lib/redis': Permission denied

/usr/bin/find: '/var/lib/sudo/ts': Permission denied

/usr/bin/find: '/var/lib/aziot/identityd': Permission denied

/usr/bin/find: '/var/lib/aziot/tpmd': Permission denied
/usr/bin/find: '/var/lib/aziot/keyd': Permission denied
/usr/bin/find: '/var/lib/aziot/certd'
: Permission denied

/usr/bin/find: '/var/log/apache2': Permission denied

/usr/bin/find:
'/var/log/redis': Permission denied

/usr/bin/find: '/var/spool/cron/crontabs': Permission denied

/usr/bin/find: '/var/spool/rsyslog': Permission [...]
```

4.1.13 Ensure successful file system mounts are collected - auditctl mount

Info

Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user
Rationale:
It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T4.5.4
NIAV2	GS1

NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep mounts' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.13 Ensure successful file system mounts are collected - mounts

Info

Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user
Rationale:
It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T4.5.4
NIAV2	GS1

NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.14 Ensure file deletion events by users are collected - auditctl delete

Info

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier 'delete'.
Rationale:
Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
At a minimum, configure the audit system to collect file deletion events for all users and root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-171	3.13.1
800-53	AU-3
800-53	AU-12
800-53	SC-7(10)
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CN-L3	8.1.10.6(j)
CSCV7	13
CSCV7	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.13.1.3
ITSG-33	AU-3
ITSG-33	AU-12
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T3.6.2
NESA	T4.5.4
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep delete' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.14 Ensure file deletion events by users are collected - delete

Info

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier 'delete'.
Rationale:
Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
At a minimum, configure the audit system to collect file deletion events for all users and root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-171	3.13.1
800-53	AU-3
800-53	AU-12
800-53	SC-7(10)
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CN-L3	8.1.10.6(j)
CSCV7	13
CSCV7	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.13.1.3
ITSG-33	AU-3
ITSG-33	AU-12
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T3.6.2
NESA	T4.5.4
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.15 Ensure changes to system administration scope (sudoers) is collected - /etc/sudoers

Info

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier 'scope.'
Rationale:
Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Solution

Add the following line to the /etc/audit/audit.rules file:
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e

NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.15 Ensure changes to system administration scope (sudoers) is collected - /etc/sudoers.d/

Info

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier 'scope.'
Rationale:
Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Solution

Add the following line to the /etc/audit/audit.rules file:
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e

NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.15 Ensure changes to system administration scope (sudoers) is collected - auditctl /etc/sudoers

Info

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier 'scope.'
Rationale:
Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Solution

Add the following line to the /etc/audit/audit.rules file:
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e

NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep scope' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.15 Ensure changes to system administration scope (sudoers) is collected - auditctl /etc/sudoers.d/

Info

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier 'scope.'
Rationale:
Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Solution

Add the following line to the /etc/audit/audit.rules file:
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d

NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep scope' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.16 Ensure system administrator actions (sudolog) are collected - /var/log/sudo.log

Info

Monitor the sudo log file. If the system has been properly configured to disable the use of the su command and force all administrators to have to log in first and then use sudo to execute privileged commands, then all administrator commands will be logged to /var/log/sudo.log . Any time a command is executed, an audit event will be triggered as the /var/log/sudo.log file will be opened for write and the executed administration command will be written to the log.
Rationale:
Changes in /var/log/sudo.log indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to /var/log/sudo.log to verify if unauthorized commands have been executed.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/sudo.log -p wa -k actions
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The system must be configured with su disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through sudo. This will not be effective on the console, as administrators can log in as root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.16 Ensure system administrator actions (sudolog) are collected - auditctl /var/log/sudo.log

Info

Monitor the sudo log file. If the system has been properly configured to disable the use of the su command and force all administrators to have to log in first and then use sudo to execute privileged commands, then all administrator commands will be logged to /var/log/sudo.log . Any time a command is executed, an audit event will be triggered as the /var/log/sudo.log file will be opened for write and the executed administration command will be written to the log.
Rationale:
Changes in /var/log/sudo.log indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to /var/log/sudo.log to verify if unauthorized commands have been executed.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/sudo.log -p wa -k actions
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The system must be configured with su disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through sudo. This will not be effective on the console, as administrators can log in as root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep actions' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.17 Ensure kernel module loading and unloading is collected - /sbin/insmod

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.17 Ensure kernel module loading and unloading is collected - /sbin/modprobe

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.17 Ensure kernel module loading and unloading is collected - /sbin/rmmod

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.17 Ensure kernel module loading and unloading is collected - auditctl /sbin/insmod

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep modules' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.17 Ensure kernel module loading and unloading is collected - auditctl /sbin/modprobe

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep modules' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.17 Ensure kernel module loading and unloading is collected - auditctl /sbin/rmmod

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep modules' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.17 Ensure kernel module loading and unloading is collected - auditctl init_module

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep modules' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.17 Ensure kernel module loading and unloading is collected - init_module

Info

Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of 'modules'.
Rationale:
Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.18 Ensure the audit configuration is immutable

Info

Set system audit so that audit rules cannot be modified with auditctl . Setting the flag '-e 2' forces audit to be put in immutable mode. Audit changes can only be made on system reboot.
Rationale:
In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Solution

Add the following line to the end of the /etc/audit/audit.rules file.
-e 2
Notes:
This setting will ensure reloading the auditd config to set active settings requires a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

/bin/grep: /etc/audit/audit.rules: No such file or directory
```

4.1.2 Ensure auditd service is enabled

Info

Turn on the auditd daemon to record system events.
Rationale:
The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Solution

Run the following command to enable auditd:
systemctl enable auditd

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	9.1
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

4.1.3 Ensure auditing for processes that start prior to auditd is enabled

Info

Configure grub so that processes that are capable of being audited can be audited even if they start up prior to auditd startup.
Rationale:
Audit events need to be captured on processes that start up prior to auditd, so that potential malicious activity cannot go undetected.

Solution

Edit /etc/default/grub and add audit=1 to GRUB_CMDLINE_LINUX:
GRUB_CMDLINE_LINUX='audit=1'
Run the following command to update the grub2 configuration:
update-grub
Notes:
This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	2S
NESA	T3.6.2

NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^[[:space:]]*linux' /boot/grub/grub.cfg' returned :

/bin/grep:
/boot/grub/grub.cfg
: No such file or directory
```

4.1.4 Ensure events that modify date and time information are collected - /etc/localtime

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.4 Ensure events that modify date and time information are collected - adjtimex settimeofday stime

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.4 Ensure events that modify date and time information are collected - auditctl /etc/localtime

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep time-change' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.4 Ensure events that modify date and time information are collected - auditctl adjtimex

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep time-change' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.4 Ensure events that modify date and time information are collected - auditctl clock_settime

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep time-change' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.4 Ensure events that modify date and time information are collected - clock_settime

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - /etc/group

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - /etc/gshadow

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - /etc/passwd

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - /etc/security/opasswd

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - /etc/shadow

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.5 Ensure events that modify user/group information are collected - auditctl /etc/group

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep identity' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.5 Ensure events that modify user/group information are collected - auditctl /etc/gshadow

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep identity' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.5 Ensure events that modify user/group information are collected - auditctl /etc/passwd

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep identity' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.5 Ensure events that modify user/group information are collected - auditctl /etc/security/opasswd

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep identity' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.5 Ensure events that modify user/group information are collected - auditctl /etc/shadow

Info

Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier 'identity' in the audit log file.
Rationale:
Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	4.8
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c

NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep identity' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - /etc/hosts

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.6 Ensure events that modify the system's network environment are collected - /etc/issue

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.6 Ensure events that modify the system's network environment are collected - /etc/sysconfig/network

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.6 Ensure events that modify the system's network environment are collected - auditctl '/etc/hosts'

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep system-locale' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - auditctl '/etc/issue'

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep system-locale' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - auditctl '/etc/network'

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep system-locale' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - auditctl 'issue.net'

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep system-locale' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - auditctl 'sethostname setdomainname'

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep system-locale' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.6 Ensure events that modify the system's network environment are collected - issue.net

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.6 Ensure events that modify the system's network environment are collected - sethostname setdomainname

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.8 Ensure login and logout events are collected - auditctl faillog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep logins' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.8 Ensure login and logout events are collected - auditctl lastlog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep logins' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.8 Ensure login and logout events are collected - auditctl tallylog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep logins' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.8 Ensure login and logout events are collected - faillog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.8 Ensure login and logout events are collected - lastlog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.8 Ensure login and logout events are collected - tallylog

Info

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 module
Rationale:
Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.9 Ensure session initiation information is collected - /var/log/btmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.9 Ensure session initiation information is collected - /var/log/wtmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.9 Ensure session initiation information is collected - /var/run/utmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/audit/audit.rules
```

4.1.9 Ensure session initiation information is collected - auditctl /var/log/btmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep logins' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.9 Ensure session initiation information is collected - auditctl /var/log/wtmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep logins' returned :

bash: /sbin/auditctl: No such file or directory
```

4.1.9 Ensure session initiation information is collected - auditctl /var/run/utmp

Info

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier 'session.' The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier 'logins.'
Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Solution

Add the following lines to the /etc/audit/audit.rules file:
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
The last command can be used to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-171	3.1.10
800-171	3.3.1
800-171	3.3.2
800-53	AC-2(12)
800-53	AC-11
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.2(d)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.1(b)
CN-L3	8.1.4.3(b)
CSCV7	4.9
CSCV7	16.11
CSCV7	16.13
CSF	DE.CM-1
CSF	DE.CM-3

CSF	PR.AC-1
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(a)(2)(iii)
HIPAA	164.312(b)
ISO/IEC-27001	A.9.2.1
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-2
ITSG-33	AC-11
ITSG-33	AU-3
LEVEL	2S
NESA	M5.3.1
NESA	T3.6.2
NIAV2	AM23c
NIAV2	AM23d
NIAV2	AM28
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2

QCSC-V1	15.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/auditctl -l | /bin/grep session' returned :

bash: /sbin/auditctl: No such file or directory
```

4.2.1.1 Ensure rsyslog Service is enabled

Info

Once the rsyslog package is installed it needs to be activated.
Rationale:
If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.

Solution

Run the following command to enable rsyslog:
systemctl enable rsyslog

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	9.1
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b

NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/systemctl is-enabled rsyslog | /usr/bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

disabled
```

4.2.1.2 Ensure logging is configured - '*.*;mail.none;news.none -/var/log/messages'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*\*\.\*;mail.none;news\.none' /etc/rsyslog.conf /etc/rsyslog.d/*.conf'
 did not return any result
```

4.2.1.2 Ensure logging is configured - '*.=warning;*.=err -/var/log/warn'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*\*\.=warning;\*\.=err' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not
 return any result
```

4.2.1.2 Ensure logging is configured - '*.crit /var/log/warn'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*\*\.crit' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any
 result
```

4.2.1.2 Ensure logging is configured - 'local0,local1.* -/var/log/localmessages'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*local0,local1' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.2 Ensure logging is configured - 'local2,local3.* -/var/log/localmessages'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*local2,local3' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.2 Ensure logging is configured - 'local4,local5.* -/var/log/localmessages'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*local4,local5' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.2 Ensure logging is configured - 'local6,local7.* -/var/log/localmessages'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*local6,local7' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.2 Ensure logging is configured - 'mail.* -/var/log/mail'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*mail\.\*' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :

/etc/rsyslog.conf:mail.*    -/var/log/mail.log
```

4.2.1.2 Ensure logging is configured - 'mail.warning -/var/log/mail.warn'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*mail\.warning' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.2 Ensure logging is configured - 'news.crit -/var/log/news/news.crit'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*news\.crit' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any
 result
```

4.2.1.2 Ensure logging is configured - 'news.err -/var/log/news/news.err'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*news\.err' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any
 result
```

4.2.1.2 Ensure logging is configured - 'news.notice -/var/log/news/news.notice'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*news\.notice' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Info

The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead.
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).
. @@loghost.example.com
Run the following command to reload the rsyslogd configuration:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.
Notes:
The double 'at' sign (@@) directs rsyslog to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-6
CN-L3	7.1.3.3(d)
CSCV7	6.6
CSCV7	6.8
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
LEVEL	1S
NESA	M5.2.5
QCSC-V1	5.2.3

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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts - InputTCPServerRun 514

Info

By default, rsyslog does not listen for log messages coming in from remote systems. The ModLoad tells rsyslog to load the imtcp.so module so it can listen over a network via TCP. The InputTCPServerRun option instructs rsyslogd to listen on the specified TCP port.
Rationale:
The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Solution

For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and un-comment or add the following lines:
$ModLoad imtcp $InputTCPServerRun 514
For hosts that are not designated as log hosts, edit the /etc/rsyslog.conf file and comment or remove the following lines:
$ModLoad imtcp # $InputTCPServerRun 514
Run the following command to reload the rsyslogd configuration:
pkill -HUP rsyslogd
References:
See the rsyslog(8) man page for more information.
Notes:
The $MoadLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2

CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '\$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not
 return any result
```

4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts - ModLoad imtcp

Info

By default, rsyslog does not listen for log messages coming in from remote systems. The ModLoad tells rsyslog to load the imtcp.so module so it can listen over a network via TCP. The InputTCPServerRun option instructs rsyslogd to listen on the specified TCP port.
Rationale:
The guidance in the section ensures that remote log hosts are configured to only accept rsyslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote rsyslog messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Solution

For hosts that are designated as log hosts, edit the /etc/rsyslog.conf file and un-comment or add the following lines:
$ModLoad imtcp $InputTCPServerRun 514
For hosts that are not designated as log hosts, edit the /etc/rsyslog.conf file and comment or remove the following lines:
$ModLoad imtcp # $InputTCPServerRun 514
Run the following command to reload the rsyslogd configuration:
pkill -HUP rsyslogd
References:
See the rsyslog(8) man page for more information.
Notes:
The $MoadLoad imtcp line can have the .so extension added to the end of the module, or use the full path to the module.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3

CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '\$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return
 any result
```

4.2.4 Ensure permissions on all logfiles are configured

Info

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.
Rationale:
It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Solution

Run the following command to set permissions on all existing log files:
chmod -R g-wx,o-rwx /var/log/*
Notes:
You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.
Some software or environments may re-set the permissions on these files. Site policy should dictate the appropriate setting for your implementation.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-171	3.4.2
800-53	AU-6
800-53	CM-6
CN-L3	7.1.3.3(d)
CSCV6	3.1
CSCV7	5.1
CSCV7	6
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.IP-1
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
ITSG-33	CM-6

LEVEL	1S
NESA	M5.2.5
QCSC-V1	5.2.3
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'OUTPUT=$(ls -l /var/log); /usr/bin/find /var/log -type f -perm /g+wx,o+rwx -ls
 | /bin/awk -v awkvar="${OUTPUT}" '{print} END {if (NR == 0) print awkvar "\npass" ; else print
 "fail"}'' returned :

bash: /bin/awk: No such file or directory

/usr/bin/find: '/var/log/apache2': Permission denied
```

5.1.2 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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/crontab
```

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/cron.hourly
```

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/cron.daily
```

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/cron.weekly
```

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/cron.monthly
```

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

/etc/cron.d
```

5.1.8 Ensure at/cron is restricted to authorized users - at.allow

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow, cron jobs can still be run as that user. The cron.allow file 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

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow:
rm /etc/cron.deny # rm /etc/at.deny # touch /etc/cron.allow # touch /etc/at.allow # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV6	3.1
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/at.allow
```

5.1.8 Ensure at/cron is restricted to authorized users - cron.allow

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow, cron jobs can still be run as that user. The cron.allow file 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

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow:
rm /etc/cron.deny # rm /etc/at.deny # touch /etc/cron.allow # touch /etc/at.allow # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV6	3.1
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/cron.allow
```

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Info

The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.
Rationale:
The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Solution

Run the following commands to set ownership and permissions on /etc/ssh/sshd_config:
chown root:root /etc/ssh/sshd_config # chmod og-rwx /etc/ssh/sshd_config

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/ssh/sshd_config with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/ssh/sshd_config
```

5.2.10 Ensure SSH root login is disabled

Info

The PermitRootLogin parameter specifies if the root user can log in using ssh. The default is no.
Rationale:
Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su. This in turn 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 as follows:
PermitRootLogin no
Default Value:
PermitRootLogin without-password

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
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-2
LEVEL	1S
NIAV2	AM16
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitRootLogin(?-i)[\s]"
```

5.2.11 Ensure SSH 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 as follows:
PermitEmptyPasswords no
Default Value:
PermitEmptyPasswords no

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
CSCV7	16.3
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
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitEmptyPasswords(?-i)[\s]"
```

5.2.12 Ensure SSH 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 as follows:
PermitUserEnvironment no
Default Value:
PermitUserEnvironment no

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)PermitUserEnvironment(?-i)[\s]"
```

5.2.13 Ensure only strong ciphers are used

Info

This variable limits the ciphers that SSH can use during communication.
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 DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a 'Sweet32' attack
The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the 'Bar Mitzvah' issue
The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session
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 plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors
The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers Example:
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
Default Value:
Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
References:
https://nvd.nist.gov/vuln/detail/CVE-2016-2183
https://nvd.nist.gov/vuln/detail/CVE-2015-2808
https://www.kb.cert.org/vuls/id/565052
https://www.openssh.com/txt/cbc.adv
https://nvd.nist.gov/vuln/detail/CVE-2008-5161
https://nvd.nist.gov/vuln/detail/CVE-2013-4548
https://www.kb.cert.org/vuls/id/565052
https://www.openssh.com/txt/cbc.adv
SSHD_CONFIG(5)
Notes:
Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.
The only ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr
CVE-2013-4548 referenced above applies to OpenSSH versions 6.2 and 6.3. If running these versions of Open SSH, Please upgrade to version 6.4 or later to fix the vulnerability, or disable AES-GCM in the server configuration.
The Following are the supported ciphers in openSSH:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
chacha20-poly1305@openssh.com

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.8
800-53	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
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
CSF	PR.DS-2
CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29

NIAV2	SS24
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep ciphers | /bin/grep -oP '((3des-cbc|aes128-cbc|
aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbcz|rijndael-
cbc@lysator.liu.se)[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }''
 returned :

bash: /bin/awk: No such file or directory

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

5.2.14 Ensure only strong MAC algorithms are used

Info

This variable limits the types of MAC algorithms that SSH can use during communication.
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
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example:
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256
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,hmac-sha1-etm@openssh.com
References:
More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH
SSHD_CONFIG(5)
Notes:
Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.
The only MACs currently FIPS 140-2 approved are hmac-sha2-256 and hmac-sha2-512
The Supported MACs are:
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-171	3.13.8
800-53	IA-5
800-53	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
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
CSF	PR.AC-1
CSF	PR.DS-2
CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	IA-5
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T5.2.3
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29

NIAV2	SS24
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep -i 'MACs' | /bin/grep -oP '((hmac-md5|hmac-md5-96|
hmac-ripemd160|hmac-sha1|hmac-sha1-96|hmac-sha1-96|umac-64@openssh.com|umac-128@openssh.com|
hmac-md5-etm@openssh.com|hmac-md5-96-etm@openssh.com|hmac-ripemd160-etm@openssh.com|hmac-sha1-
etm@openssh.com|hmac-sha1-96-etm@openssh.com|umac-64-etm@openssh.com|umac-128-etm@openssh.com)
[,]?)+' | /bin/awk '{print} END {if (NR == 0) print "pass"; else print $0 }'' returned :

bash: /bin/awk: No such file or directory

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

5.2.15 Ensure only strong Key Exchange algorithms are used

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
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
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example:
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
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-group14-sha1,diffie-hellman-group1-sha1
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
The Key Exchange algorithms supported by OpenSSH 7 are:
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.8
800-53	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
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
CSF	PR.DS-2

CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2
NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep -i 'kexalgorithms' | /bin/grep -oP '((diffie-hellman-
group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)[,]?)+' | /bin/awk
 '{print} END {if (NR == 0) print "pass"; else print $0 }'' returned :

bash: /bin/awk: No such file or directory

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

5.2.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveInterval

Info

The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time.
Rationale:
Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..
While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Solution

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:
ClientAliveInterval 300
ClientAliveCountMax 0
Default Value:
ClientAliveInterval 300
ClientAliveCountMax 0

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.10
800-53	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	1S
NIAV2	AM23c
NIAV2	AM23d

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep clientaliveinterval' returned :

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

```
clientaliveinterval 0
```

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

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 as follows:
LoginGraceTime 60
Default Value:
LoginGraceTime 120

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep logingracetime' returned :

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
logingracetime 120
```

5.2.18 Ensure SSH access is limited

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 as follows:
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)(Allow|Deny)(Users|Groups)(?-i)[\s]"
```

5.2.19 Ensure SSH warning 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 as follows:
Banner /etc/issue.net

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)Banner(?-i)[\s]"
```

5.2.4 Ensure SSH Protocol is set to 2

Info

Older versions of SSH support two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.
Rationale:
SSH v1 suffers from insecurities that do not affect SSH v2.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter as follows:
Protocol 2
Notes:
This command not longer exists in newer versions of SSH. This check is still being included for systems that may be running an older version of SSH. As of openSSH version 7.4 this parameter will not cause an issue when included.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.8
800-53	SC-8
CN-L3	8.1.2.2(a)
CN-L3	8.1.2.2(b)
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
CSF	PR.DS-2
CSF	PR.DS-5
GDPR	32.1.a
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(e)(1)
HIPAA	164.312(e)(2)(i)
ITSG-33	SC-8
ITSG-33	SC-8a.
LEVEL	1S
NESA	T4.3.1
NESA	T4.3.2

NESA	T4.5.1
NESA	T4.5.2
NESA	T7.3.3
NESA	T7.4.1
NIAV2	IE8
NIAV2	IE9
NIAV2	IE12
NIAV2	NS29
NIAV2	SS24
QCSC-V1	5.2.2
QCSC-V1	6.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)Protocol(?-i)[\s]"
```

5.2.5 Ensure SSH LogLevel is appropriate

Info

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.
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.
Rationale:
SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter as follows:
LogLevel VERBOSE
OR
LogLevel INFO
Default Value:
LogLevel INFO
References:
https://www.ssh.com/ssh/sshd_config/

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3

ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)LogLevel(?-i)[\s]"
```

5.2.6 Ensure SSH X11 forwarding is disabled

Info

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.
Rationale:
Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter as follows:
X11Forwarding no

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	3.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/ssh/sshd_config - regex '^[\s]*(?i)X11Forwarding(?-i)[\s]' found - expect '^[\s]*(?
i)X11Forwarding(?-i)[\s]+no[\s]*$' not found in the following lines:
          89: X11Forwarding yes
```

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

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 as follows:
MaxAuthTries 4
Default Value:
MaxAuthTries 6

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.2
800-53	AC-2(12)
CN-L3	7.1.3.2(d)
CSCV6	16.7
CSCV7	16.13
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-2
LEVEL	1S
NESA	M5.3.1
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)MaxAuthTries(?-i)[\s]"
```

5.2.8 Ensure SSH 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 as follows:
IgnoreRhosts yes
Default Value:
IgnoreRhosts yes

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)IgnoreRhosts(?-i)[\s]"
```

5.2.9 Ensure SSH 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. This option only applies to SSH Protocol Version 2.
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 as follows:
HostbasedAuthentication no
Default Value:
HostbasedAuthentication no

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	AC-14a.
800-53	IA-5
CSCV7	16.3
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	AC-14a.
ITSG-33	IA-5
LEVEL	1S
NESA	T5.2.3
NESA	T5.6.1
QCSC-V1	5.2.2
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/ssh/sshd_config" does not contain "^[\s]*(?i)HostbasedAuthentication(?-i)[\s]"
```

5.3.1 Ensure password creation requirements are configured - dcredit

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

5.3.1 Ensure password creation requirements are configured - lcredit

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

5.3.1 Ensure password creation requirements are configured - minlen

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

5.3.1 Ensure password creation requirements are configured - ocredit

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

5.3.1 Ensure password creation requirements are configured - retry=3

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV6	16.7
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1 4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/pam.d/common-password" does not contain
 "^[\s]*password[\s]+requisite[\s]+pam_pwquality\.so[\s]"
```

5.3.1 Ensure password creation requirements are configured - ucredit

Info

The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.
The following are definitions of the pam_pwquality.so options.
retry=3 - Allow 3 tries before sending back a failure.
The following options are set in the /etc/security/pwquality.conf file:
minlen = 14 - password must be 14 characters or more
dcredit = -1 - provide at least one digit
ucredit = -1 - provide at least one uppercase character
ocredit = -1 - provide at least one special character
lcredit = -1 - provide at least one lowercase character
The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.
Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Solution

Run the following command to install the pam_pwquality module:
apt-get install libpam-pwquality
Edit the /etc/pam.d/common-password file to include the appropriate options for pam_pwquality.so and to conform to site policy:
password requisite pam_pwquality.so retry=3
Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:
minlen = 14 dcredit = -1 ucredit = -1 ocredit = -1 lcredit = -1
Notes:
Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.
Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

5.3.2 Ensure lockout for failed password attempts is configured

Info

Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.
Set the lockout number to the policy in effect at your site.
Rationale:
Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Edit the /etc/pam.d/common-auth file and add the auth line below:
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
Edit the /etc/pam.d/common-account file and add the account line bellow:
account required pam_tally.so
Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.
Notes:
BUG In pam_tally2.so
To work around this issue the addition of tam_tally2.so in the accounts section of the /etc/pam.d/common-account file has been added to the audit and remediation sections. pam_tally2 line must be added for the counter to reset to 0 when using sudo
Use of the 'audit' keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV6	16.7
CSCV7	16.7
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-2
LEVEL	1S
NIAV2	AM28

NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/pam.d/common-auth" does not contain
 "^[\s]*auth[\s]+required[\s]+pam_tally2\.so[\s]*"
```

5.3.3 Ensure password reuse is limited

Info

The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.
Rationale:
Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.
Note that these change only apply to accounts configured on the local system.

Solution

Edit the /etc/pam.d/common-password file to include the remember option and conform to site policy as shown:
password required pam_pwhistory.so remember=5
Notes:
Additional module options may be set, recommendation only covers those listed here.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/pam.d/common-password" does not contain
 "^[\s]*password[\s]*required[\s]*pam_pwhistory\.so"
```

5.4.1.1 Ensure password expiration is 365 days or less - login.defs

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.

Solution

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :
PASS_MAX_DAYS 90
Modify user parameters for all users with a password set to match:
chage --maxdays 90 <user>
Notes:
You can also check this setting in /etc/shadow directly. The 5th field should be 365 or less for all users with a password.
Note: A value of -1 will disable password expiration. Additionally the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)

LEVEL	1S
NESA	T5.2.3
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_MAX_DAYS[\s]' found - expect
 '^[\s]*PASS_MAX_DAYS[\s]+([1-9]|[1-8][0-9]|9[0-9]|[12][0-9]{2}|3[0-5][0-9]|36[0-5])[\s]*$' not
 found in the following lines:
         160: PASS_MAX_DAYS 99999
```

5.4.1.2 Ensure minimum days between password changes is 7 or more - login.defs

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days.
Rationale:
By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs :
PASS_MIN_DAYS 7
Modify user parameters for all users with a password set to match:
chage --mindays 7 <user>
Notes:
You can also check this setting in /etc/shadow directly. The 4th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Non-compliant file(s):
      /etc/login.defs - regex '^[\s\t]*PASS_MIN_DAYS[\s]+' found - expect 'PASS_MIN_DAYS[\s]+(?:
[1-9]|[1-9][0-9]+)(?:[\s]*|[\s]+\#?.*)$' not found in the following lines:
          161: PASS_MIN_DAYS 0
```

5.4.1.4 Ensure inactive password lock is 30 days or less - useradd

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>
Notes:
You can also check this setting in /etc/shadow directly. The 7th field should be 30 or less for all users with a password.
Note: A value of -1 would disable this setting.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV6	16.1
CSCV6	16.6
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)

LEVEL	1S
NESA	T5.2.3
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

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

INACTIVE=-1
```

5.4.2 Ensure system accounts are non-login

Info

There are a number of accounts provided with Debian that are used to manage applications and 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, Debian sets 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 /usr/sbin/nologin. Some built-in accounts use /bin/false which is also acceptable. This prevents the account from potentially being used to run any commands.

Solution

Set the shell for any accounts returned by the audit script to /usr/sbin/nologin:
usermod -s /usr/sbin/nologin <user>
passwd -l <user>
The following script will automatically set all user shells required to /usr/sbin/nologin and lock the sync, shutdown, and halt users:
#!/bin/bash
for user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [$user != 'root']; then usermod -L $user if [$user != 'sync'] && [$user != 'shutdown'] && [$user != 'halt']; then usermod -s /usr/sbin/nologin $user fi fi done

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
File : /etc/passwd, Invalid line : systemd-timesync:x:100:102:systemd Time Synchronization,,,:/
run/systemd:/bin/false
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/bash.bashrc

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.
Rationale:
Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:
umask 027
Notes:
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 default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b

QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/bash.bashrc" does not contain "^[\s]*umask[\s]"
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/profile

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.
Rationale:
Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:
umask 027
Notes:
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 default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b

QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/profile" does not contain "^[\s]*umask[\s]"
```

5.4.5 Ensure default user shell timeout is 900 seconds or less - /etc/bashrc

Info

The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds.
Rationale:
Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Solution

Edit the /etc/bash.bashrc, /etc/profile, and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any TMOUT parameters as follows:
TMOUT=600
Notes:
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.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.10
800-53	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	2S
NIAV2	AM23c
NIAV2	AM23d

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/bashrc
```

5.4.5 Ensure default user shell timeout is 900 seconds or less - /etc/profile

Info

The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds.
Rationale:
Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Solution

Edit the /etc/bash.bashrc, /etc/profile, and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any TMOUT parameters as follows:
TMOUT=600
Notes:
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.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.10
800-53	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	2S
NIAV2	AM23c
NIAV2	AM23d

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/profile" does not contain "^[\s]*TMOUT[\s]*=[\s]*"
```

5.4.5 Ensure default user shell timeout is 900 seconds or less - /etc/profile.d/*.sh

Info

The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds.
Rationale:
Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Solution

Edit the /etc/bash.bashrc, /etc/profile, and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any TMOUT parameters as follows:
TMOUT=600
Notes:
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.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.10
800-53	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	2S
NIAV2	AM23c
NIAV2	AM23d

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/profile.d/*.sh
```

5.5 Ensure root login is restricted to system console

Info

The file /etc/securetty contains a list of valid terminals that may be logged in directly as root.
Rationale:
Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Solution

Remove entries for any consoles that are not in a physically secure location.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2(9)
CN-L3	8.1.4.2(c)
CSCV7	4.3
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-2
LEVEL	1NS
NIAV2	AM16
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
 The command returned :

# /etc/securetty: list of terminals on which root is allowed to login.
# See securetty(5) and login(1).


# Local X displays (allows empty passwords with pam_unix's nullok_secure)
:0
:0.0
:0.1
```

```
:1
:1.0
:1.1
:2
:2.0
:2.1
:3
:3.0
:3.1
#...


# ============================================================
#
# TTYs sorted by major number according to Documentation/devices.txt
#
# ============================================================

tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
tty12
tty13
tty14
tty15
tty16
tty17
tty18
tty19
tty20
tty21
tty22
tty23
tty24
tty25
tty26
tty27
tty28
tty29
tty30
tty31
tty32
tty33
tty34
tty35
tty36
tty37
tty38
tty39
tty40
tty41
tty42
tty43
tty44
tty45
tty46
tty47
tty48
tty49
tty50
tty51
tty52
tty53
tty54
tty55
tty56
tty57
```

```
tty58
tty59
tty60
tty61
tty62
tty63

# UART serial ports
ttyS0
ttyS1
ttyS2
ttyS3
ttyS4
ttyS5
#...ttyS191

# Serial Mux devices (Linux/PA-RISC only)
ttyB0
ttyB1
#...

# Chase serial card
ttyH0
ttyH1
#...

# Cyclades serial cards
ttyC0
ttyC1
#...ttyC31

# Digiboard serial cards
ttyD0
ttyD1
#...

# Stallion serial cards
ttyE0
ttyE1
#...ttyE255

# Specialix serial cards
ttyX0
ttyX1
#...

# Comtrol Rocketport serial cards
ttyR0
ttyR1
#...

# SDL RISCom serial cards
ttyL0
ttyL1
#...

# Hayes ESP serial card
ttyP0
ttyP1
#...

# Computone IntelliPort II serial card
ttyF0
ttyF1
#...ttyF255

# Specialix IO8+ serial card
ttyW0
ttyW1
#...

# Comtrol VS-1000 serial controller
ttyV0
ttyV1
#...
```

```
# ISI serial card
ttyM0
ttyM1
#...

# Technology Concepts serial card
ttyT0
ttyT1
#...

# Specialix RIO serial card
ttySR0
ttySR1
#...ttySR511

# Chase Research AT/PCI-Fast serial card
ttyCH0
ttyCH1
#...ttyCH63

# Moxa Intellio serial card
ttyMX0
ttyMX1
#...ttyMX127

# SmartIO serial card
ttySI0
ttySI1
#...

# USB dongles
ttyUSB0
ttyUSB1
ttyUSB2
#...

# LinkUp Systems L72xx UARTs
ttyLU0
ttyLU1
ttyLU2
ttyLU3

# StrongARM builtin serial ports
ttySA0
ttySA1
ttySA2

# SCI serial port (SuperH) ports and SC26xx serial [...]
```

5.6 Ensure access to the su command is restricted - /etc/group

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 the sudo group to execute su.
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

Add the following line to the /etc/pam.d/su file:
auth required pam_wheel.so
Create a comma separated list of users in the sudo statement in the /etc/group file:
sudo:x:10:root,<user list>
Notes:
The use_uid option to pam_wheel.so is a no-op on debian based systems. It is acceptable but not required as these systems use its behavior as default.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep sudo: /etc/group' returned :

sudo:x:27:moxa
```

5.6 Ensure access to the su command is restricted - /etc/pam.d/su

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 the sudo group to execute su.
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

Add the following line to the /etc/pam.d/su file:
auth required pam_wheel.so
Create a comma separated list of users in the sudo statement in the /etc/group file:
sudo:x:10:root,<user list>
Notes:
The use_uid option to pam_wheel.so is a no-op on debian based systems. It is acceptable but not required as these systems use its behavior as default.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/pam.d/su" does not contain "^[\s]*auth[\s]+required[\s]+pam_wheel\.so[\s]*$"
```

6.1.1 Audit system file permissions

Info

The Debian package manager has a number of useful options. One of these, the --verify option, can be used to verify that system packages are correctly installed. The --verify option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:
Code Meaning
S File size differs.
M File mode differs (includes permissions and file type).
5 The MD5 checksum differs.
D The major and minor version numbers differ on a device file.
L A mismatch occurs in a link.
U The file ownership differs.
G The file group owner differs.
T The file time (mtime) differs.
The dpkg -S command can be used to determine which package a particular file belongs to. For example the following commands determines which package the /bin/bash file belongs to:
dpkg -S /bin/bash
bash: /bin/bash
To verify the settings for the package that controls the /bin/bash file, run the following:
dpkg --verify bash
??5?????? c /etc/bash.bashrc
Rationale:
It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Solution

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.
Notes:
Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.
Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2NS
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
 The command returned :

dpkg: warning: ppp: unable to open /etc/chatscripts/gprs for hash: Permission denied

dpkg: warning: ppp: unable to open /etc/chatscripts/pap for hash: Permission denied

dpkg: warning: sudo: unable to open /etc/sudoers for hash: Permission denied

dpkg: warning: sudo: unable to open /etc/sudoers.d/README for hash: Permission denied

dpkg: warning: snmpd: unable to open /etc/snmp/snmpd.conf for hash: Permission denied

dpkg: warning: aziot-edge: unable to open /etc/aziot/config.toml.edge.template for hash:
 Permission denied

dpkg: warning: aziot-edge: unable to open /etc/aziot/edged/config.toml.default for hash:
 Permission denied

dpkg: warning: lldpd: unable to open /usr/sbin/lldpcli for hash: Permission denied

dpkg: warning: wvdial: unable to open /etc/ppp/peers/wvdial-pipe for hash: Permission denied

dpkg: warning: wvdial: unable to open /etc/ppp/peers/wvdial for hash: Permission denied

dpkg: warning: aziot-identity-service: unable to open /etc/aziot/certd/config.toml.default for
 hash: Permission denied
```

```
dpkg: warning: aziot-identity-service: unable to open /etc/aziot/config.toml.template for hash:
 Permission denied

dpkg: warning: aziot-identity-service: unable to open /etc/aziot/identityd/config.toml.default for
 hash: Permission denied

dpkg: warning: aziot-identity-service: unable to open /etc/aziot/keyd/config.toml.default for
 hash: Permission denied

dpkg: warning: aziot-identity-service: unable to open /etc/aziot/tpmd/config.toml.default for
 hash: Permission denied

dpkg: warning: redis-server: unable to open /etc/redis/redis.conf for hash: Permission denied
??5??????   /usr/share/man/man8/ping.8.gz
??5??????   /usr/share/locale/ar/LC_MESSAGES/Linux-PAM.mo
??5??????   /usr/share/locale/as/LC_MESSAGES/Linux-PAM.mo
??5??????   /usr/share/locale/ast/LC_MESSAGES/Linux-PAM.mo
??5??????   /usr/share/locale/bal/LC_MESSAGES/Linux-PAM.mo
??5??????   /usr/share/locale/bg/LC_MESSAGES/Linux-PAM.mo
??5??????   /usr/share/locale/bn/LC_MESSAGES/Linux-PAM.mo
??5??????   [...]
```

6.1.10 Ensure no world writable files exist

Info

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information.
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.

Solution

Removing write access for the 'other' category (chmod o-w <filename>) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.5
800-53	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)
CSCV7	14
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	1S
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
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
 The following 164 files are world writeable:

  /boot_device/p2/lower/var/bruno/apps/azureiotedge/approot/postinst
     owner: root, group: root, permissions: 0777

  /boot_device/p2/lower/var/bruno/apps/azureiotedge/approot/postrm
     owner: root, group: root, permissions: 0777

  /boot_device/p2/lower/var/bruno/apps/azureiotedge/approot/poststop
     owner: root, group: root, permissions: 0777

  /boot_device/p2/lower/var/bruno/apps/azureiotedge/approot/prestart
     owner: root, group: root, permissions: 0777

  /boot_device/p2/lower/var/bruno/apps/dlmclient/approot/postinst
     owner: root, group: root, permissions: 0777

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/AWS_Simple_Icons_AWS_Cloud.svg
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/app-icon.png
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/eip-logo.png
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-page/en.json
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-page/zh-cn.json
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-page/zh-tw.json
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-password-policy-page/
en.json
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-password-policy-page/zh-
cn.json
     owner: root, group: root, permissions: 0666

  /boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/account-password-policy-page/zh-
tw.json
```

```
   owner: root, group: root, permissions: 0666

/boot_device/p2/lower/var/bruno/apps/edge-web/ui/assets/i18n/aid-page/en.json
   owner: root, group: root, permissions: 0666

[...]
```

Audits SKIPPED

Audits PASSED

1.1.1.1 Ensure mounting of freevxfs filesystems is disabled - lsmod

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/freevxfs.conf and add the following line:
install freevxfs /bin/true
Run the following command to unload the freevxfs module:
rmmod freevxfs

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/lsmod | /bin/grep freevxfs | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

bash: /usr/sbin/lsmod: No such file or directory
pass
```

1.1.1.2 Ensure mounting of jffs2 filesystems is disabled - lsmod

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/jffs2.conf and add the following line:
install jffs2 /bin/true
Run the following command to unload the jffs2 module:
rmmod jffs2

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep jffs2 | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.1.1.3 Ensure mounting of hfs filesystems is disabled - lsmod

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line:
install hfs /bin/true
Run the following command to unload the hfs module:
rmmod hfs

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep hfs | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

1.1.1.4 Ensure mounting of hfsplus filesystems is disabled - lsmod

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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfsplus.conf and add the following line:
install hfsplus /bin/true
Run the following command to unload the hfsplus module:
rmmod hfsplus

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep hfsplus | /usr/bin/awk '{print} END {if (NR == 0) print
 "pass" ; else print "fail"}'' returned :

pass
```

1.1.1.5 Ensure mounting of udf filesystems is disabled - lsmod

Info

The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.
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

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line:
install udf /bin/true
Run the following command to unload the udf module:
rmmod udf

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep udf | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

1.1.15 Ensure nodev option set on /dev/shm partition

Info

The nodev mount option specifies that the filesystem cannot contain special devices.
Rationale:
Since the /run/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

Edit the /etc/fstabfile and add nodev to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information.
Run the following command to remount /dev/shm:
mount -o remount,nodev /dev/shm

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
```

1.1.16 Ensure nosuid option set on /dev/shm partition

Info

The nosuidmount 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

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.
Run the following command to remount /dev/shm:
mount -o remount,nosuid /dev/shm

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/mount | /bin/grep /dev/shm' returned :

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
```

1.1.21 Ensure sticky bit is set on all world-writable directories

Info

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:
This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.

Solution

Run the following command to set the sticky bit on all world writable directories:
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -perm -0002 2>/dev/null | xargs chmod a+t
Notes:
Some distributions may not support the --local option to df.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/df --local -P | /usr/bin/awk {'if (NR!=1) print $6'} | /usr/bin/xargs -I '{}' /
usr/bin/find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | /usr/bin/awk
 '{print} END {if (NR == 0) print "none"}'' returned :

none
```

1.1.22 Disable Automounting

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.

Solution

Run the following command to disable autofs:
systemctl disable autofs
Impact:
The use 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.
Notes:
This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.2
800-171	3.14.4
800-171	3.14.5
800-53	SI-3
CN-L3	7.1.3.6(b)
CN-L3	8.1.4.5
CN-L3	8.1.9.6(a)
CN-L3	8.1.9.6(b)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.7(a)
CN-L3	8.1.10.7(b)
CSCV6	9.1
CSCV7	8.4
CSCV7	8.5
CSF	DE.CM-4
CSF	DE.DP-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.2.1

ITSG-33	SI-3
LEVEL	2S
NIAV2	GS8a
QCSC-V1	3.2
QCSC-V1	5.2.3
QCSC-V1	8.2.1
TBA-FIISB	49.2.1
TBA-FIISB	49.2.2
TBA-FIISB	49.3.1
TBA-FIISB	49.3.2
TBA-FIISB	50.2.1
TBA-FIISB	51.2.4
TBA-FIISB	51.2.7

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

1.5.1 Ensure core dumps are restricted - sysctl

Info

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

Solution

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file:
* hard core 0
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
fs.suid_dumpable = 0
Run the following command to set the active kernel parameter:
sysctl -w fs.suid_dumpable=0

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl fs.suid_dumpable' returned :

fs.suid_dumpable = 0
```

1.5.3 Ensure address space layout randomization (ASLR) is enabled - sysctl

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 /etc/sysctl.d/* file:
kernel.randomize_va_space = 2
Run the following command to set the active kernel parameter:
sysctl -w kernel.randomize_va_space=2

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	SC-39
800-53	SI-16
CSCV6	3.1
CSCV7	8.3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1S
QCSC-V1	5.2.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl kernel.randomize_va_space' returned :

kernel.randomize_va_space = 2
```

1.5.4 Ensure prelink is disabled

Info

prelink is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.
Rationale:
The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.

Solution

Run the following command to restore binaries to normal:
prelink -ua
Run the following command to uninstall prelink:
apt-get remove prelink

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g

QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s prelink 2>&1' returned :

dpkg-query: package 'prelink' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

1.6.1.4 Ensure no unconfined daemons exist

Info

Daemons that are not defined in SELinux policy will inherit the security context of their parent process.
Rationale:
Since daemons are launched and descend from the init process, they will inherit the security context label initrc_t. This could cause the unintended consequence of giving the process more permission than it requires.

Solution

Investigate any unconfined daemons found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.
Notes:
Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	2S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

none
```

1.7.1.1 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, or v. , or references to the OS platform

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No matching files were found
```

1.7.1.4 Ensure permissions on /etc/motd are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/motd:
chown root:root /etc/motd # chmod 644 /etc/motd

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/motd with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/motd
```

1.7.1.5 Ensure permissions on /etc/issue are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/issue:
chown root:root /etc/issue # chmod 644 /etc/issue

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/issue with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/issue
```

1.7.1.6 Ensure permissions on /etc/issue.net are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Solution

Run the following commands to set permissions on /etc/issue.net:
chown root:root /etc/issue.net # chmod 644 /etc/issue.net

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/issue.net with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/issue.net
```

1.7.2 Ensure GDM login banner is configured - banner message enabled

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

Edit or create the file /etc/gdm3/greeter.dconf-defaults and add the following:
[org/gnome/login-screen] banner-message-enable=true banner-message-text='Authorized uses only. All activity may be monitored and reported.'
Notes:
Additional options and sections may appear in the /etc/dconf/db/gdm.d/01-banner-message file.
If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

1.7.2 Ensure GDM login banner is configured - banner text

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

Edit or create the file /etc/gdm3/greeter.dconf-defaults and add the following:
[org/gnome/login-screen] banner-message-enable=true banner-message-text='Authorized uses only. All activity may be monitored and reported.'
Notes:
Additional options and sections may appear in the /etc/dconf/db/gdm.d/01-banner-message file.
If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

1.8 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.
Notes:
Site policy may mandate a testing period before install onto production systems for available updates.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.1
800-53	SI-2c.
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
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b

QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/apt-get -s upgrade | /bin/egrep -v '(Reading|Building|Calculating)''
 returned :

NOTE: This is only a simulation!
      apt-get needs root privileges for real execution.
      Keep also in mind that locking is deactivated,
      so don't depend on the relevance to the real current situation!
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

2.1.1 Ensure xinetd is not installed

Info

The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.
Rationale:
If there are no xinetd services required, it is recommended that the package be removed.

Solution

Run the following commands to remove xinetd:
apt-get remove xinetd
apt-get purge xinetd
Notes:
Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s xinetd 2>&1' returned :

dpkg-query: package 'xinetd' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.1.2 Ensure openbsd-inetd is not installed

Info

The inetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.
Rationale:
If there are no inetd services required, it is recommended that the daemon be removed.

Solution

Run the following command to uninstall openbsd-inetd:
apt-get remove openbsd-inetd

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1

CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s openbsd-inetd 2>&1' returned :

dpkg-query: package 'openbsd-inetd' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.2.1.1 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.
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

On physical systems or virtual systems where host based time synchronization is not available install NTP or chrony using one of the following commands:
apt-get install ntp # apt-get install chrony
On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1NS
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

2.2.1.2 Ensure ntp is configured - RUNASUSER

Info

ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.
This recommendation only applies if ntp is in use on the system.
Rationale:
If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Solution

Add or edit restrict lines in /etc/ntp.conf to match the following:
restrict -4 default kod nomodify notrap nopeer noquery restrict -6 default kod nomodify notrap nopeer noquery
Add or edit server or pool lines to /etc/ntp.conf as appropriate:
server <remote-server>
Configure ntp to run as the ntp user by adding or editing the /etc/init.d/ntp file:
RUNASUSER=ntp

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV6	3.1
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Compliant file(s):
      /etc/init.d/ntp - regex '^[\s]*RUNASUSER[\s]*=' found - expect
 '^[\s]*RUNASUSER[\s]*=[\s]*ntp[\s]*$' found in the following lines:
         32: RUNASUSER=ntp
```

2.2.1.3 Ensure chrony is configured

Info

chrony is a daemon which implements the Network Time Protocol (NTP) 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.
This recommendation only applies if chrony is in use on the system.

Solution

Add or edit server or pool lines to /etc/chrony/chrony.conf as appropriate:
server <remote-server>

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.7
800-53	AU-8
CN-L3	8.1.4.3(b)
CSCV7	6.1
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-8
LEVEL	1S
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
TBA-FIISB	37.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

2.2.10 Ensure HTTP server is not enabled

Info

HTTP or web servers provide the ability to host web site content.
Rationale:
Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Solution

Run the following command to disable apache2:
systemctl disable apache2

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

disabled
```

2.2.11 Ensure IMAP and POP3 server is not enabled

Info

exim is an open source IMAP and POP3 server 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.

Solution

Run the following commands to remove exim:
apt-get remove exim4
apt-get purge exim4
Notes:
Several IMAP/POP3 servers exist and can use other service names. dovecot and cyrus-imap are example services that provide a mail server. These and other services should also be audited.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s exim4' returned :

dpkg-query: package 'exim4' is not installed and no information is available

Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.2.12 Ensure Samba is not enabled

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 Small 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 service can be deleted to reduce the potential attack surface.

Solution

Run the following command to disable smbd:
systemctl disable smbd

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.2.13 Ensure HTTP Proxy Server is not enabled

Info

Squid is a standard proxy server used in many distributions and environments.
Rationale:
If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Solution

Run the following command to disable squid:
systemctl disable squid

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.2.14 Ensure SNMP Server is not enabled

Info

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 SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to disallow SNMP v1.

Solution

Run the following command to disable snmpd:
systemctl disable snmpd
Notes:
Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1

CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

disabled
```

2.2.15 Ensure mail transfer agent is configured for local-only mode - /etc/postfix/main.cf

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
Restart postfix:
systemctl restart postfix
Notes:
This recommendation 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/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	3.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3

CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

2.2.15 Ensure mail transfer agent is configured for local-only mode - netstat

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
Restart postfix:
systemctl restart postfix
Notes:
This recommendation 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/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4

CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

2.2.17 Ensure NIS Server is not enabled

Info

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.
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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used

Solution

Run the following command to disable nis:
systemctl disable nis

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s nis | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'nis' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.2.3 Ensure Avahi Server is not enabled

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 disable the service to reduce the potential attach surface.

Solution

Run the following command to disable avahi-daemon:
systemctl disable avahi-daemon

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

Failed to get unit file state for avahi-daemon.service: No such file or directory
disabled
```

2.2.4 Ensure CUPS is not enabled

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 disabled to reduce the potential attack surface.

Solution

Run the following command to disable cups:
systemctl disable cups
Impact:
Disabling CUPS will prevent printing from the system, a common task for workstation systems.
References:
More detailed documentation on CUPS is available at the project homepage at http://www.cups.org.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1

CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	2S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.2.5 Ensure DHCP Server is not enabled - dhcpd

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.
Rationale:
Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be disabled to reduce the potential attack surface.

Solution

Run the following commands to disable dhcpd:
systemctl disable isc-dhcp-server # systemctl disable isc-dhcp-server6
References:
More detailed documentation on DHCP is available at http://www.isc.org/software/dhcp.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

Failed to get unit file state for isc-dhcp-server.service: No such file or directory
disabled
```

2.2.5 Ensure DHCP Server is not enabled - isc-dhcp-server6

Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.
Rationale:
Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be disabled to reduce the potential attack surface.

Solution

Run the following commands to disable dhcpd:
systemctl disable isc-dhcp-server # systemctl disable isc-dhcp-server6
References:
More detailed documentation on DHCP is available at http://www.isc.org/software/dhcp.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

Failed to get unit file state for isc-dhcp-server6.service: No such file or directory
disabled
```

2.2.6 Ensure LDAP server is not enabled

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.
Rationale:
If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.

Solution

Run the following command to disable slapd:
systemctl disable slapd
References:
For more detailed documentation on OpenLDAP, go to the project homepage at http://www.openldap.org.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.2.7 Ensure NFS and RPC are not enabled - nfs-server

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 export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.

Solution

Run the following commands to disable nfs and rpcbind:
systemctl disable nfs-server # systemctl disable rpcbind

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

Failed to get unit file state for nfs-server.service: No such file or directory
disabled
```

2.2.7 Ensure NFS and RPC are not enabled - rpcbind

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 export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.

Solution

Run the following commands to disable nfs and rpcbind:
systemctl disable nfs-server # systemctl disable rpcbind

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.2.8 Ensure DNS Server is not enabled

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 deleted to reduce the potential attack surface.

Solution

Run the following command to disable named:
systemctl disable bind9

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

Failed to get unit file state for bind9.service: No such file or directory
disabled
```

2.2.9 Ensure FTP Server is not enabled

Info

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.
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 deleted to reduce the potential attack surface.

Solution

Run the following command to disable vsftpd:
systemctl disable vsftpd
Notes:
Additional FTP servers also exist and should be audited.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV6	9.1
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

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

2.3.1 Ensure NIS Client is not installed

Info

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (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.

Solution

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-53	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s nis 2>&1' returned :

dpkg-query: package 'nis' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.3.2 Ensure rsh client is not installed - rsh-client

Info

The rshpackage contains the client commands for the rsh services.
Rationale:
These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the rshpackage removes the clients for rsh, rcpand rlogin.

Solution

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.5.3
800-53	CM-11
800-53	IA-2(1)
CN-L3	7.1.2.7(b)
CSCV7	2.6
CSCV7	4.5
CSF	DE.CM-3
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.12.6.2
ITSG-33	IA-2(1)
LEVEL	1S
NESA	T5.4.2
NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s rsh-client 2>&1' returned :

dpkg-query: package 'rsh-client' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.3.2 Ensure rsh client is not installed - rsh-redone-client

Info

The rshpackage contains the client commands for the rsh services.
Rationale:
These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the rshpackage removes the clients for rsh, rcpand rlogin.

Solution

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.5.3
800-53	CM-11
800-53	IA-2(1)
CN-L3	7.1.2.7(b)
CSCV7	2.6
CSCV7	4.5
CSF	DE.CM-3
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.12.6.2
ITSG-33	IA-2(1)
LEVEL	1S
NESA	T5.4.2
NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s rsh-redone-client 2>&1' returned :

dpkg-query: package 'rsh-redone-client' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.3.3 Ensure talk client is not installed

Info

The talk software makes it possible for users to send and receive messages across systems through a terminal session. The talk client, which allows initialization of talk sessions, is installed by default.
Rationale:
The software presents a security risk as it uses unencrypted protocols for communication.

Solution

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-53	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s talk 2>&1' returned :

dpkg-query: package 'talk' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

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.

Solution

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

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-171	3.5.3
800-53	CM-11
800-53	IA-2(1)
CN-L3	7.1.2.7(b)
CSCV7	2.6
CSCV7	4.5
CSF	DE.CM-3
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.12.6.2
ITSG-33	IA-2(1)
LEVEL	1S
NESA	T5.4.2
NIAV2	AM36
NIAV2	VL3c
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
SWIFT-CSCV1	1.2
SWIFT-CSCV1	5.1
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s telnet 2>&1' returned :

dpkg-query: package 'telnet' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

2.3.5 Ensure LDAP client is not installed

Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.
Rationale:
If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Solution

Uninstall ldap-utils using the appropriate package manager or manual installation:
apt-get remove ldap-utils
Impact:
Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.9
800-53	CM-11
CSCV7	2.6
CSF	DE.CM-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.2
LEVEL	1S
QCSC-V1	8.2.1
SWIFT-CSCV1	5.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s ldap-utils 2>&1' returned :

dpkg-query: package 'ldap-utils' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
```

3.1.1 Ensure IP forwarding is disabled - ipv6 sysctl

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 the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Solution

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.ip_forward=0 # sysctl -w net.ipv6.conf.all.forwarding=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.all.forwarding' returned :

net.ipv6.conf.all.forwarding = 0
```

3.2.1 Ensure source routed packets are not accepted - net.ipv4.conf.all.accept_source_route = 0

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.accept_source_route' returned :

net.ipv4.conf.all.accept_source_route = 0
```

3.2.1 Ensure source routed packets are not accepted - net.ipv6.conf.all.accept_source_route = 0

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.all.accept_source_route' returned :

net.ipv6.conf.all.accept_source_route = 0
```

3.2.1 Ensure source routed packets are not accepted - net.ipv6.conf.default.accept_source_route = 0

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 /etc/sysctl.d/* file:
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
Run the following commands 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.ipv6.conf.all.accept_source_route=0 # sysctl -w net.ipv6.conf.default.accept_source_route=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv6.conf.default.accept_source_route' returned :

net.ipv6.conf.default.accept_source_route = 0
```

3.2.2 Ensure ICMP redirects are not accepted - net.ipv4.conf.all.accept_redirects

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. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.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.
Rationale:
Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0
Run the following commands 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.ipv6.conf.all.accept_redirects=0 # sysctl -w net.ipv6.conf.default.accept_redirects=0 # sysctl -w net.ipv4.route.flush=1 # sysctl -w net.ipv6.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.conf.all.accept_redirects' returned :

net.ipv4.conf.all.accept_redirects = 0
```

3.2.5 Ensure broadcast ICMP requests are ignored - net.ipv4.icmp_echo_ignore_broadcasts = 1

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 parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.icmp_echo_ignore_broadcasts = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts' returned :

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

3.2.6 Ensure bogus ICMP responses are ignored - net.ipv4.icmp_ignore_bogus_error_responses = 1

Info

Setting 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 /etc/sysctl.d/* file:
net.ipv4.icmp_ignore_bogus_error_responses = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses' returned :

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

3.2.8 Ensure TCP SYN Cookies is enabled - net.ipv4.tcp_syncookies = 1

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. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Solution

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.tcp_syncookies = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.tcp_syncookies=1 # sysctl -w net.ipv4.route.flush=1

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.2
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/sysctl net.ipv4.tcp_syncookies' returned :

net.ipv4.tcp_syncookies = 1
```

3.3.4 Ensure permissions on /etc/hosts.allow are configured

Info

The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate.
Rationale:
It is critical to ensure that the /etc/hosts.allow 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 set permissions on /etc/hosts.allow:
chown root:root /etc/hosts.allow # chmod 644 /etc/hosts.allow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/hosts.allow with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/hosts.allow
```

3.3.5 Ensure permissions on /etc/hosts.deny are configured

Info

The /etc/hosts.deny file contains network information that is used by many system applications and therefore must be readable for these applications to operate.
Rationale:
It is critical to ensure that the /etc/hosts.deny 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 set permissions on /etc/hosts.deny :
chown root:root /etc/hosts.deny # chmod 644 /etc/hosts.deny

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/hosts.deny with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/hosts.deny
```

3.4.1 Ensure DCCP is disabled - lsmod

Info

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.
Rationale:
If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/dccp.conf and add the following line:
install dccp /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep dccp | /usr/bin/awk '{print} END {if (NR == 0) print "pass" ;
 else print "fail"}'' returned :

pass
```

3.4.2 Ensure SCTP is disabled - lsmod

Info

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/sctp.conf and add the following line:
install sctp /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5

CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep sctp | /usr/bin/awk '{print} END {if (NR == 0) print "pass";
 else print "fail"}'' returned :

pass
```

3.4.3 Ensure RDS is disabled - lsmod

Info

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/rds.conf and add the following line:
install rds /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep rds | /usr/bin/awk '{print} END {if (NR == 0) print "pass";
 else print "fail"}'' returned :

pass
```

3.4.4 Ensure TIPC is disabled - lsmod

Info

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.
Rationale:
If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Solution

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/tipc.conf and add the following line:
install tipc /bin/true

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8

CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/lsmod | /bin/grep tipc | /usr/bin/awk '{print} END {if (NR == 0) print "pass";
 else print "fail"}'' returned :

pass
```

3.5.3 Ensure iptables is installed

Info

iptables allows configuration of the IPv4 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to iptables.
Rationale:
iptables is required for firewall management and configuration.

Solution

Run the following command to install iptables:
apt-get install iptables

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV6	9.2
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/dpkg -s iptables 2>&1' returned :

Package: iptables
Status: install ok installed
Priority: important
Section: net
Installed-Size: 1113
Maintainer: Arturo Borrero Gonzalez <arturo@debian.org>
Architecture: armhf
Multi-Arch: foreign
Version: 1.6.0+snapshot20161117-6
Depends: libip4tc0 (= 1.6.0+snapshot20161117-6), libip6tc0 (= 1.6.0+snapshot20161117-6), libiptc0
 (= 1.6.0+snapshot20161117-6), libxtables12 (= 1.6.0+snapshot20161117-6), libc6 (>= 2.7),
 libnetfilter-conntrack3, libnfnetlink0
Suggests: kmod
Description: administration tools for packet filtering and NAT
 iptables is the userspace command line program used to configure
 the Linux packet filtering ruleset. It is targeted towards system
 administrators. Since Network Address Translation is also configured
 from the packet filter ruleset, iptables is used for this, too. The
 iptables package also includes ip6tables. ip6tables is used for
 configuring the IPv6 packet filter
Homepage: http://www.netfilter.org/
```

3.6 Ensure wireless interfaces are disabled

Info

Wireless networking is used when wired networks are unavailable. Debian contains a wireless tool kit to allow system administrators to configure and use wireless networks.
Rationale:
If wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the following command to disable any wireless interfaces:
ip link set <interface> down
Disable any wireless interfaces in your network configuration.
Impact:
Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.16
800-53	AC-18(3)
CSCV6	15.8
CSCV7	15.4
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ITSG-33	AC-18(3)
LEVEL	2NS
QCSC-V1	5.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/iwconfig | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'' returned :

bash: /sbin/iwconfig: No such file or directory
none
```

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl chmod fchmod fchmodat x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl chown fchown fchownat lchown x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.10 Ensure discretionary access control permission modification events are collected - auditctl setxattr x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.10 Ensure discretionary access control permission modification events are collected - chmod fchmod fchmodat x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.10 Ensure discretionary access control permission modification events are collected - chown fchown fchownat lchown x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.10 Ensure discretionary access control permission modification events are collected - lsetxattr setxattr fsetxattr removexattr x64

Info

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier 'perm_mod.'
Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EACCES x64

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EPERM x64

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EACCES x64

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - auditctl EPERM x64

Info

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier 'access.'
Rationale:
Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	14.9
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
LEVEL	2S

NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.13 Ensure successful file system mounts are collected - auditctl mount x64

Info

Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user
Rationale:
It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T4.5.4
NIAV2	GS1

NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.13 Ensure successful file system mounts are collected - mounts x64

Info

Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user
Rationale:
It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T4.5.4
NIAV2	GS1

NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.14 Ensure file deletion events by users are collected - auditctl delete x64

Info

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier 'delete'.
Rationale:
Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
At a minimum, configure the audit system to collect file deletion events for all users and root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-171	3.13.1
800-53	AU-3
800-53	AU-12
800-53	SC-7(10)
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CN-L3	8.1.10.6(j)
CSCV7	13
CSCV7	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.13.1.3
ITSG-33	AU-3
ITSG-33	AU-12
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T3.6.2
NESA	T4.5.4
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.14 Ensure file deletion events by users are collected - delete x64

Info

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier 'delete'.
Rationale:
Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
At a minimum, configure the audit system to collect file deletion events for all users and root.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-171	3.13.1
800-53	AU-3
800-53	AU-12
800-53	SC-7(10)
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CN-L3	8.1.10.6(j)
CSCV7	13
CSCV7	6.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.AC-5

CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.13.1.3
ITSG-33	AU-3
ITSG-33	AU-12
ITSG-33	SC-7(10)
LEVEL	2S
NESA	T3.6.2
NESA	T4.5.4
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.4 Ensure events that modify date and time information are collected - auditctl clock_settime x64

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.4 Ensure events that modify date and time information are collected - auditctl settimeofday,adjtimex x64

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.4 Ensure events that modify date and time information are collected - clock_settime x64

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.4 Ensure events that modify date and time information are collected - settimeofday,adjtimex x64

Info

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier 'time-change'
Rationale:
Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.6 Ensure events that modify the system's network environment are collected - auditctl 'sethostname setdomainname' x64

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.6 Ensure events that modify the system's network environment are collected - sethostname setdomainname x64

Info

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses) and /etc/network (directory containing network interface scripts and configurations) files.
Rationale:
Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/network is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised.
All audit records will be tagged with the identifier 'system-locale.'

Solution

For 32 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
/etc/network is common Debian based distributions.
Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as /etc/sysconfig/network.
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - /etc/apparmor

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - /etc/apparmor.d

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - /etc/selinux

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - /usr/share/selinux

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /etc/apparmor

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /etc/apparmor.d

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /etc/selinux

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected - auditctl /usr/share/selinux

Info

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.
Rationale:
Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Solution

On systems using SELinux add the following line to the /etc/audit/audit.rules file:
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
On systems using AppArmor add the following line to the /etc/audit/audit.rules file:
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
Impact:
Auditing can produce a large amount of information, creating large and/or many audit log files.
Notes:
Reloading the auditd config to set active settings may require a system reboot.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.5
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	2S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

4.2.1.2 Ensure logging is configured - '*.emerg :omusrmsg:*'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*\*\.emerg' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :

/etc/rsyslog.conf:*.emerg    :omusrmsg:*
```

4.2.1.2 Ensure logging is configured - 'mail.err /var/log/mail.err'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*mail\.err' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :

/etc/rsyslog.conf:mail.err   /var/log/mail.err
```

4.2.1.2 Ensure logging is configured - 'mail.info -/var/log/mail.info'

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:
.emerg :omusrmsg: mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err news.crit -/var/log/news/news.crit news.err -/var/log/news/news.err news.notice -/var/log/news/news.notice
.=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:
pkill -HUP rsyslogd
References:
See the rsyslog.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12

LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep '^s*mail\.info' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :

/etc/rsyslog.conf:mail.info   -/var/log/mail.info
```

4.2.1.3 Ensure rsyslog default file permissions 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.

Solution

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set $FileCreateMode to 0640 or more restrictive:
$FileCreateMode 0640
References:
See the rsyslog.conf(5) man page for more information.
Notes:
You should also ensure this is not overridden with less restrictive settings in any /etc/rsyslog.d/* conf file.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :

/etc/rsyslog.conf:$FileCreateMode 0640
```

4.2.2.1 Ensure syslog-ng service is enabled

Info

Once the syslog-ng package is installed it needs to be activated.
Rationale:
If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.

Solution

Run the following command to enable syslog-ng:
update-rc.d syslog-ng enable

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV6	9.1
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b

NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.2.2 Ensure logging is configured

Info

The /etc/syslog-ng/syslog-ng.conf file 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 syslog-ng (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the log lines in the /etc/syslog-ng/syslog-ng.conf file as appropriate for your environment:
log { source(src); source(chroots); filter(f_console); destination(console); };
log { source(src); source(chroots); filter(f_console); destination(xconsole); };
log { source(src); source(chroots); filter(f_newscrit); destination(newscrit); };
log { source(src); source(chroots); filter(f_newserr); destination(newserr); };
log { source(src); source(chroots); filter(f_newsnotice); destination(newsnotice); };
log { source(src); source(chroots); filter(f_mailinfo); destination(mailinfo); };
log { source(src); source(chroots); filter(f_mailwarn); destination(mailwarn); };
log { source(src); source(chroots); filter(f_mailerr); destination(mailerr); };
log { source(src); source(chroots); filter(f_mail); destination(mail); };
log { source(src); source(chroots); filter(f_acpid); destination(acpid); flags(final); };
log { source(src); source(chroots); filter(f_acpid_full); destination(devnull); flags(final); };
log { source(src); source(chroots); filter(f_acpid_old); destination(acpid); flags(final); };
log { source(src); source(chroots); filter(f_netmgm); destination(netmgm); flags(final); };
log { source(src); source(chroots); filter(f_local); destination(localmessages); };
log { source(src); source(chroots); filter(f_messages); destination(messages); };
log { source(src); source(chroots); filter(f_iptables); destination(firewall); };
log { source(src); source(chroots); filter(f_warn); destination(warn); };
Run the following command to reload the syslog-ng configuration:
pkill -HUP syslog-ng
References:
See the syslog-ng man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7

CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1NS
NESA	T3.6.2
NIAV2	AM34a
NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.2.3 Ensure syslog-ng default file permissions configured

Info

syslog-ng 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 exist and have the correct permissions to ensure that sensitive syslog-ng data is archived and protected.

Solution

Edit the /etc/syslog-ng/syslog-ng.conf and set perm option to 0640 or more restrictive:
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600); threaded(yes); };
References:
See the syslog-ng man pages for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.2.4 Ensure syslog-ng is configured to send logs to a remote log host - destination logserver

Info

The syslog-ng utility supports the ability to send logs it gathers to a remote log host or to receive messages from remote hosts, reducing administrative overhead.
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/syslog-ng/syslog-ng.conf file and add the following lines (where logfile.example.com is the name of your central log host).
destination logserver { tcp('logfile.example.com' port(514)); };
log { source(src); destination(logserver); };
Run the following command to reload the syslog-ng configuration:
pkill -HUP syslog-ng
References:
See the syslog-ng.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-6
CN-L3	7.1.3.3(d)
CSCV7	6.6
CSCV7	6.8
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
LEVEL	1NS
NESA	M5.2.5
QCSC-V1	5.2.3
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.2.4 Ensure syslog-ng is configured to send logs to a remote log host - log src

Info

The syslog-ng utility supports the ability to send logs it gathers to a remote log host or to receive messages from remote hosts, reducing administrative overhead.
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/syslog-ng/syslog-ng.conf file and add the following lines (where logfile.example.com is the name of your central log host).
destination logserver { tcp('logfile.example.com' port(514)); };
log { source(src); destination(logserver); };
Run the following command to reload the syslog-ng configuration:
pkill -HUP syslog-ng
References:
See the syslog-ng.conf(5) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-6
CN-L3	7.1.3.3(d)
CSCV7	6.6
CSCV7	6.8
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.DP-4
CSF	PR.PT-1
CSF	RS.AN-1
CSF	RS.CO-2
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-6
LEVEL	1NS
NESA	M5.2.5
QCSC-V1	5.2.3
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.2.5 Ensure remote syslog-ng messages are only accepted on designated log hosts

Info

By default, syslog-ng does not listen for log messages coming in from remote systems.
Rationale:
The guidance in the section ensures that remote log hosts are configured to only accept syslog-ng data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote syslog-ng messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Solution

On designated log hosts edit the /etc/syslog-ng/syslog-ng.conf file and configure the following lines are appropriately:
source net{ tcp(); };
destination remote { file('/var/log/remote/${FULLHOST}-log'); };
log { source(net); destination(remote); };
On non designated log hosts edit the /etc/syslog-ng/syslog-ng.conf file and remove or edit any sources that accept network sourced log messages.
Run the following command to reload the syslog-ng configuration:
pkill -HUP syslog-ng
References:
See the syslog-ng(8) man page for more information.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.14.6
800-171	3.14.7
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CSCV7	9.2
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2
CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5

CSF	ID.RA-1
CSF	PR.DS-5
CSF	PR.IP-8
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	SI-4
LEVEL	1NS
NESA	M1.2.2
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

4.2.3 Ensure rsyslog or syslog-ng is installed

Info

The rsyslog and syslog-ng software are recommended replacements to the original syslogd daemon which provide improvements over syslogd, 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.
Rationale:
The security enhancements of rsyslog and syslog-ng 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

Install rsyslog or syslog-ng using one of the following commands:
apt-get install rsyslog # apt-get install syslog-ng

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.3.1
800-171	3.3.2
800-53	AU-3
800-53	AU-12
CN-L3	7.1.2.3(a)
CN-L3	7.1.2.3(b)
CN-L3	7.1.3.3(a)
CN-L3	8.1.4.3(b)
CSCV7	6.2
CSCV7	6.3
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.PT-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-3
ITSG-33	AU-12
LEVEL	1S
NESA	T3.6.2
NIAV2	AM34a

NIAV2	AM34b
NIAV2	AM34c
NIAV2	AM34d
NIAV2	AM34e
NIAV2	AM34f
NIAV2	AM34g
QCSC-V1	3.2
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	13.2
SWIFT-CSCV1	6.4

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

5.1.1 Ensure cron daemon is enabled

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

Run the following command to enable cron:
systemctl enable cron

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

enabled
```

5.1.8 Ensure at/cron is restricted to authorized users - at.deny

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow, cron jobs can still be run as that user. The cron.allow file 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

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow:
rm /etc/cron.deny # rm /etc/at.deny # touch /etc/cron.allow # touch /etc/at.allow # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV6	9.1
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/at.deny
```

5.1.8 Ensure at/cron is restricted to authorized users - cron.deny

Info

Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow, cron jobs can still be run as that user. The cron.allow file 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

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow:
rm /etc/cron.deny # rm /etc/at.deny # touch /etc/cron.allow # touch /etc/at.allow # chmod og-rwx /etc/cron.allow # chmod og-rwx /etc/at.allow # chown root:root /etc/cron.allow # chown root:root /etc/at.allow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV6	9.1
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1

QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No files found: /etc/cron.deny
```

5.2.16 Ensure SSH Idle Timeout Interval is configured - ClientAliveCountMax

Info

The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time.
Rationale:
Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..
While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Solution

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:
ClientAliveInterval 300
ClientAliveCountMax 0
Default Value:
ClientAliveInterval 300
ClientAliveCountMax 0

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.10
800-53	AC-11
CN-L3	8.1.4.1(b)
CSCV7	16.11
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ISO/IEC-27001	A.11.2.8
ITSG-33	AC-11
LEVEL	1S
NIAV2	AM23c
NIAV2	AM23d

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/sbin/sshd -T | /bin/grep clientalivecountmax' returned :

Could not load host key: /etc/ssh/ssh_host_rsa_key

Could not load host key: /etc/ssh/ssh_host_ecdsa_key

Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

```
clientalivecountmax 3
```

5.2.2 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 commands to set ownership and permissions on the private SSH host key files
find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {} ;
find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod 0600 {} ;

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/ssh/ssh_host_ecdsa_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_ed25519_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_rsa_key with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/ssh/ssh_host_ecdsa_key, /etc/ssh/ssh_host_ed25519_key, /etc/ssh/ssh_host_rsa_key
```

5.2.3 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 commands to set permissions and ownership on the SSH host public key files
find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod 0644 {} ;
#find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root {} ;

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/ssh/ssh_host_ecdsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid:
 0 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_ed25519_key.pub with fmode owner: root group: root mode: 0644 uid: 0
 gid: 0 uneven permissions : FALSE is compliant with the policy value
The file /etc/ssh/ssh_host_rsa_key.pub with fmode owner: root group: root mode: 0644 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/ssh/ssh_host_ecdsa_key.pub, /etc/ssh/ssh_host_ed25519_key.pub, /etc/ssh/ssh_host_rsa_key.pub
```

5.3.4 Ensure password hashing algorithm is SHA-512

Info

The commands below change password encryption from md5 to sha512 (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.
Rationale:
The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.
Note that these change only apply to accounts configured on the local system.

Solution

Edit the /etc/pam.d/common-password file to include the sha512 option for pam_unix.so as shown:
password [success=1 default=ignore] pam_unix.so sha512
Notes:
Additional module options may be set, recommendation only covers those listed here.
If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.
cat /etc/passwd | awk -F: '($3 >= 1000 && $1 != 'nfsnobody') { print $1 }' | xargs -n 1 chage -d 0

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Compliant file(s):
```

```
     /etc/pam.d/common-password - regex '^password.*pam_unix.so' found - expect 'sha512' found in
the following lines:
         25: password [success=1 default=ignore] pam_unix.so obscure sha512
```

5.4.1.1 Ensure password expiration is 365 days or less - users

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.

Solution

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :
PASS_MAX_DAYS 90
Modify user parameters for all users with a password set to match:
chage --maxdays 90 <user>
Notes:
You can also check this setting in /etc/shadow directly. The 5th field should be 365 or less for all users with a password.
Note: A value of -1 will disable password expiration. Additionally the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)

LEVEL	1S
NESA	T5.2.3
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'echo 'Username, Maximum number of days between password change'; output="";
 failures=0; for i in $(egrep "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do change_date=$(chage
 --list "$i" | grep 'Maximum number of days between password change' | cut -d: -f2 | awk '{$1=
$1};1'); output="${i}, ${change_date}"; if [ $change_date -le 365 ] && [ $change_date -ge 1 ];
 then output="${output} - Pass"; else output="${output} - Fail"; failures=$((failures+1)); fi;
 echo "${output}"; done; echo "Number of failures: ${failures}"' returned :

grep: /etc/shadow: Permission denied
Username, Maximum number of days between password change
Number of failures: 0
```

5.4.1.2 Ensure minimum days between password changes is 7 or more - users

Info

The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days.
Rationale:
By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Solution

Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs :
PASS_MIN_DAYS 7
Modify user parameters for all users with a password set to match:
chage --mindays 7 <user>
Notes:
You can also check this setting in /etc/shadow directly. The 4th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'echo 'Username, Minimum number of days between password change'; output="";
 failures=0; for i in $(egrep "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do change_date=$(chage
 --list "$i" | grep 'Minimum number of days between password change' | cut -d: -f2 | awk '{$1=
$1};1'); output="${i}, ${change_date}"; if [ $change_date -ge 7 ]; then output="${output} -
 Pass"; else output="${output} - Fail"; failures=$((failures+1)); fi; echo "${output}"; done; echo
 "Number of failures: ${failures}"' returned :

grep:
/etc/shadow
: Permission denied
Username, Minimum number of days between password change
Number of failures: 0
```

5.4.1.3 Ensure password expiration warning days is 7 or more - login.defs

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>
Notes:
You can also check this setting in /etc/shadow directly. The 6th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
Compliant file(s):
      /etc/login.defs - regex '^[\s]*PASS_WARN_AGE[\s]+' found - expect
 '^[\s]*PASS_WARN_AGE[\s]+([7-9]|[1-9][0-9]+)\s*$' found in the following lines:
         162: PASS_WARN_AGE 7
```

5.4.1.3 Ensure password expiration warning days is 7 or more - users

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>
Notes:
You can also check this setting in /etc/shadow directly. The 6th field should be 7 or more for all users with a password.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3

NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'echo 'Username, Number of days of warning before password expires'; output="";
 failures=0; for i in $(egrep "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do change_date=$(chage
 --list "$i" | grep 'Number of days of warning before password expires' | cut -d: -f2 | awk
 '{$1=$1};1'); output="${i}, ${change_date}"; if [ $change_date -ge 7 ]; then output="${output} -
 Pass"; else output="${output} - Fail"; failures=$((failures+1)); fi; echo "${output}"; done; echo
 "Number of failures: ${failures}"' returned :

grep:
/etc/shadow
: Permission denied
Username, Number of days of warning before password expires
Number of failures: 0
```

5.4.1.4 Ensure inactive password lock is 30 days or less - users

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>
Notes:
You can also check this setting in /etc/shadow directly. The 7th field should be 30 or less for all users with a password.
Note: A value of -1 would disable this setting.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV6	16.1
CSCV6	16.6
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)

LEVEL	1S
NESA	T5.2.3
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'echo 'Username, Inactive password days'; output=""; failures=0; for i in $(egrep
 "^[^:]+:[^!*]" /etc/shadow | cut -d: -f1); do password_expires=$(egrep "^\b$i\b" /etc/shadow
 | cut -d: -f7 | tr -d '\n'); if [ -z "$password_expires" ]; then password_expires=-1; fi;
 output="${i}, ${password_expires}"; if [ $password_expires -le 30 ] && [ $password_expires -ge
 1 ]; then status="Pass"; else status="Fail"; failures=$((failures+1)); fi; echo "${output} -
 ${status}"; done; echo "Number of failures: ${failures}"' returned :

grep: /etc/shadow: Permission denied
Username, Inactive password days
Number of failures: 0
```

5.4.1.5 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 users 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/files/2619

References

800-171	3.1.1
800-171	3.5.2
800-53	AC-2
800-53	IA-5(1)
CN-L3	7.1.3.2(d)
CSCV7	16
CSCV7	4.4
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)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e

QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'echo 'Username, Current Days, Last Password Change Days'; output=""; failures=0;
 for i in $(cut -d: -f1 < /etc/shadow); do now=$(($(date +%s) / 86400)); change_date=
$(chage --list "$i" | grep 'Last password change' | cut -d: -f2 | awk '{$1=$1};1'); if
 [[ $change_date != "never" ]]; then epoch_change_date=$(($(date -d "${change_date}" +%s) /
 86400)); else epoch_change_date='Never'; fi; output="${i}, ${now}, ${epoch_change_date}"; if
 [[ $epoch_change_date -le $now ]]; then output="${output} - Pass"; else output="${output} -
 Fail"; ((failures++)); fi; echo "${output}"; done; echo "Number of failures: ${failures}"'
 returned :

bash: /etc/shadow: Permission denied
Username, Current Days, Last Password Change Days
Number of failures: 0
```

5.4.3 Ensure default group for the root account is GID 0

Info

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.
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 default group to GID 0:
usermod -g 0 root

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
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
```

5.4.4 Ensure default user umask is 027 or more restrictive - /etc/profile.d/*.sh

Info

The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories.
Rationale:
Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Solution

Edit the /etc/bash.bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:
umask 027
Notes:
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 default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(10)
CN-L3	8.1.10.6(j)
CSCV7	13
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(10)
LEVEL	1S
NESA	T4.5.4
NIAV2	GS1
NIAV2	GS2a
NIAV2	GS2b

QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	33.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No matching files were found
```

6.1.11 Ensure no unowned files or directories exist

Info

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.
Rationale:
A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.6
800-171	3.4.7
800-53	CM-7
CSCV7	13.2
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7
LEVEL	1S
NIAV2	SS15a
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No issues found.
```

6.1.12 Ensure no ungrouped files or directories exist

Info

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.
Rationale:
A new user who is assigned the deleted user's user ID or group ID may then end up 'owning' these files, and thus have more access on the system than was intended.

Solution

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.6
800-171	3.4.7
800-53	CM-7
CSCV7	13.2
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-7
LEVEL	1S
NIAV2	SS15a
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No issues found.
```

6.1.2 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 permissions on /etc/gshadow:
chown root:shadow /etc/gshadow # chmod o-rwx,g-wx/etc/gshadow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/gshadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow
```

6.1.3 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 one of the following chown commands as appropriate and the chmod to set permissions on /etc/shadow- :
chown root:shadow /etc/shadow-
chmod o-rwx,g-wx /etc/shadow-

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/shadow- with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow-
```

6.1.4 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 one of the following chown commands as appropriate and the chmod to set permissions on /etc/gshadow- :
chown root:shadow /etc/gshadow-
chmod o-rwx,g-wx /etc/gshadow-

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/gshadow- with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow-
```

6.1.5 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 command to set permissions on /etc/passwd:
chown root:root /etc/passwd # chmod 644 /etc/passwd

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
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
```

6.1.6 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 one following commands to set permissions on /etc/shadow:
chown root:shadow /etc/shadow # chmod o-rwx,g-wx /etc/shadow

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/shadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow
```

6.1.7 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 command to set permissions on /etc/group:
chown root:root /etc/group # chmod 644 /etc/group

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
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
```

6.1.8 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 command to set permissions on /etc/passwd- :
chown root:root /etc/passwd- # chmod u-x,go-wx /etc/passwd-

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/passwd- with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd-
```

6.1.9 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 command to set permissions on /etc/group- :
chown root:root /etc/group- # chmod u-x,go-wx /etc/group-

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	3.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file /etc/group- with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/group-
```

6.2.1 Ensure 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/files/2619

References

800-171	3.5.2
800-53	IA-5(1)
CSCV7	4.4
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	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/cat /etc/shadow | /usr/bin/awk -F : '($2 == "") { print $1 " does not have a
 password."}'| /usr/bin/awk '{print} END {if (NR == 0) print "none"'}' returned :

/bin/cat:
/etc/shadow
: Permission denied
none
```

6.2.10 Ensure users' dot files are not group or world writable

Info

While the system administrator can establish secure permissions for users' 'dot' files, the users can easily override these.
Rationale:
Group or world-writable user configuration files 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.
Notes:
On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

6.2.11 Ensure no users have .forward files

Info

The .forward file specifies an email address to forward the user's mail to.
Rationale:
Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

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 .forward files and determine the action to be taken in accordance with site policy.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	9.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

6.2.12 Ensure no users have .netrc files

Info

The .netrc file contains data for logging into a remote host for file transfers via FTP.
Rationale:
The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

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 .netrc files and determine the action to be taken in accordance with site policy.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV6	9.1
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

6.2.13 Ensure users' .netrc Files are not group or world accessible

Info

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.
Rationale:
.netrc files may contain unencrypted passwords that may be used to attack other systems.

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 .netrc file permissions and determine the action to be taken in accordance with site policy.
Notes:
While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.
On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command 'for dir in $(/usr/bin/cat /etc/passwd | /usr/bin/egrep -v '(root|halt|sync|shutdown)'
 | /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'); do if [ -f "$dir/.netrc" ]; then
 fileperm=$(ls -ld $dir/.netrc | cut -f1 -d" "); if [ $(/usr/bin/echo $fileperm | cut -c5) !=
 "-" ]; then /usr/bin/echo "Group Read set on $dir/.netrc"; fi; if [ $(/usr/bin/echo $fileperm
 | cut -c6) != "-" ]; then /usr/bin/echo "Group Write set on $dir/.netrc"; fi; if [ $(/usr/
bin/echo $fileperm | cut -c7) != "-" ]; then /usr/bin/echo "Group Execute set on $dir/.netrc";
 fi; if [ $(/usr/bin/echo $fileperm | cut -c8) != "-" ]; then /usr/bin/echo "Other Read set on
 $dir/.netrc"; fi; if [ $(/usr/bin/echo $fileperm | cut -c9) != "-" ]; then /usr/bin/echo "Other
 Write set on $dir/.netrc"; fi; if [ $(/usr/bin/echo $fileperm | cut -c10) != "-" ]; then /usr/
bin/echo "Other Execute set on $dir/.netrc"; fi; fi; done | /usr/bin/awk '{ print } END { if
 (NR==0) print "All .netrc files are not group or world accessible" }'' returned :

bash: /usr/bin/cat: No such file or directory

bash: /usr/bin/egrep: No such file or directory
All .netrc files are not group or world accessible
```

6.2.14 Ensure no users have .rhosts files

Info

While no .rhosts files are shipped by default, users can easily create them.
Rationale:
This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf. Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

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 .rhosts files and determine the action to be taken in accordance with site policy.
Notes:
On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.2
800-53	IA-5
800-53	IA-5(1)
CSCV7	16.4
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
ITSG-33	IA-5(1)
LEVEL	1S
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

bash: /usr/bin/egrep: No such file or directory

bash: /usr/bin/cat: No such file or directory
No .rhosts files found
```

6.2.15 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/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No issues found.
```

6.2.16 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/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No duplicate User IDs detected
```

6.2.17 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.
Notes:
You can also use the grpck command to check for other inconsistencies in the /etc/group file.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

No duplicate Group IDs detected

6.2.18 Ensure no duplicate user names exist

Info

Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.
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/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

No issues found.

6.2.19 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/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

No issues found.

6.2.2 Ensure no legacy '+' entries exist in /etc/passwd

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.
Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/passwd if they exist.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.1
800-53	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)
CSCV7	16.2
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-2
ITSG-33	IA-2a.
LEVEL	1S
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/passwd" does not contain "^[\s]*\+:"
```

6.2.20 Ensure shadow group is empty

Info

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.
Rationale:
Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

Solution

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-2
CN-L3	7.1.3.2(d)
CSCV7	16
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-2
LEVEL	1S
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="")
 { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1;
 f=1 } END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd' returned :

shadow group empty
```

6.2.4 Ensure no legacy '+' entries exist in /etc/group

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.
Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/group if they exist.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.1
800-53	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)
CSCV7	16.2
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-2
ITSG-33	IA-2a.
LEVEL	1S
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The file "/etc/group" does not contain "^[\s]*\+:"
```

6.2.5 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/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	5.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No issues found.
```

6.2.6 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 items discovered in the Audit step.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	8.4
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command returned :

su: must be run from a terminal

stat:
missing operand


Try 'stat --help' for more information.
No other writable paths for root interactive environment
```

6.2.7 Ensure all users' home directories exist

Info

Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.
Rationale:
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 any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV6	3.1
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/bin/cat /etc/passwd | /bin/egrep -v '^(root|halt|sync|shutdown)' | /usr/bin/awk -F:
 '($7 != "/usr/sbin/nologin" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do
 if [ ! -d "$dir" ]; then /bin/echo "The home directory ($dir) of user $user does not exist."; fi;
 done | /usr/bin/awk '{ print } END { if(NR==0) { print "No results found" } }'' returned :

No results found
```

6.2.9 Ensure users own their home directories

Info

The user home directory is space defined for the particular user to set local environment variables and to store personal files.
Rationale:
Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Solution

Change the ownership of any home directories that are not owned by the defined user to the correct user.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
No issues found.
```

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit from CIS Debian Linux 9 Benchmark

Info

See Also

https://workbench.cisecurity.org/files/2619

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit from CIS Debian Linux 9 Benchmark

Info

See Also

https://workbench.cisecurity.org/files/2619

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L2.audit

Assets

security-aig-301.itest.conn.com

Audits INFO,WARNING,ERROR

1.2.1 Ensure package manager repositories are configured

Info

Systems need to have package manager repositories configured to ensure they 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/files/2619

References

800-171	3.14.1
800-53	SI-2c.
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
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/usr/bin/apt-cache policy' returned :

Package files:
 100 /var/lib/dpkg/status
     release a=now
Pinned packages:
```

1.2.2 Ensure GPG keys are configured

Info

Most packages managers implement GPG key signing to verify package integrity during 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.
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/files/2619

References

800-171	3.14.1
800-53	SI-2c.
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
CSF	ID.RA-1
CSF	PR.IP-12
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-2
LEVEL	1NS
NESA	T7.6.2
NESA	T7.7.1
NIAV2	AM38
NIAV2	AM39
NIAV2	SS14b
QCSC-V1	11.2
SWIFT-CSCV1	2.2

Audit File

Assets

security-aig-301.itest.conn.com

```
 The command '/usr/bin/apt-key list' returned :

Warning: apt-key output should not be parsed (stdout is not a terminal)
/etc/apt/trusted.gpg.d/debian-archive-buster-automatic.gpg
----------------------------------------------------------
pub   rsa4096 2019-04-14 [SC] [expires: 2027-04-12]
      80D1 5823 B7FD 1561 F9F7  BCDD DC30 D7C2 3CBB ABEE
uid           [ unknown] Debian Archive Automatic Signing Key (10/buster) <ftpmaster@debian.org>
sub   rsa4096 2019-04-14 [S] [expires: 2027-04-12]

/etc/apt/trusted.gpg.d/debian-archive-buster-security-automatic.gpg
-------------------------------------------------------------------
pub   rsa4096 2019-04-14 [SC] [expires: 2027-04-12]
      5E61 B217 265D A980 7A23  C5FF 4DFA B270 CAA9 6DFA
uid           [ unknown] Debian Security Archive Automatic Signing Key (10/buster)
 <ftpmaster@debian.org>
sub   rsa4096 2019-04-14 [S] [expires: 2027-04-12]

/etc/apt/trusted.gpg.d/debian-archive-buster-stable.gpg
-------------------------------------------------------
pub   rsa4096 2019-02-05 [SC] [expires: 2027-02-03]
      6D33 866E DD8F FA41 C014  3AED DCC9 EFBF 77E1 1517
uid           [ unknown] Debian Stable Release Key (10/buster) <debian-release@lists.debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-automatic.gpg
----------------------------------------------------------
pub   rsa4096 2014-11-21 [SC] [expired: 2022-11-19]
      126C 0D24 BD8A 2942 CC7D  F8AC 7638 D044 2B90 D010
uid           [ expired] Debian Archive Automatic Signing Key (8/jessie) <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-security-automatic.gpg
-------------------------------------------------------------------
pub   rsa4096 2014-11-21 [SC] [expired: 2022-11-19]
      D211 6914 1CEC D440 F2EB  8DDA 9D6D 8F6B C857 C906
uid           [ expired] Debian Security Archive Automatic Signing Key (8/jessie)
 <ftpmaster@debian.org>

/etc/apt/trusted.gpg.d/debian-archive-jessie-stable.gpg
-------------------------------------------------------
pub   rsa4096 2013-08-17 [SC] [expired: [...]
```

1.4.3 Ensure authentication required for single user mode

Info

Single user mode is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.
Rationale:
Requiring authentication in single user mode prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Solution

Run the following command and follow the prompts to set a password for the root user:
passwd root

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1S
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

3.5.1.3 Ensure outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established connections.
Rationale:
If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2

QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/iptables -L -v -n' returned :

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
```

3.5.1.4 Ensure firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
Rationale:
Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:
iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.
The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-171	3.14.6
800-171	3.14.7
800-53	SC-7(12)
800-53	SI-4
CN-L3	7.1.3.5(a)
CN-L3	8.1.10.5(b)
CN-L3	8.1.10.6(f)
CN-L3	8.1.10.6(j)
CSCV7	9.2
CSCV7	9.4
CSF	DE.AE-1
CSF	DE.AE-2
CSF	DE.AE-3
CSF	DE.AE-4
CSF	DE.CM-1
CSF	DE.CM-5
CSF	DE.CM-6
CSF	DE.CM-7
CSF	DE.DP-2

CSF	DE.DP-3
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.RA-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.IP-8
CSF	PR.PT-4
CSF	RS.AN-1
CSF	RS.CO-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
ITSG-33	SI-4
LEVEL	1S
NESA	M1.2.2
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	3.2
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	5.2.3
QCSC-V1	6.2
QCSC-V1	8.2.1
QCSC-V1	10.2.1
QCSC-V1	11.2
TBA-FIISB	43.1

Audit File

Assets

security-aig-301.itest.conn.com

```
 The command '/bin/netstat -ln; /sbin/iptables -L INPUT -v -n' returned :

iptables v1.6.0: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:2947          0.0.0.0:*               LISTEN
tcp        0      0 172.31.8.1:6379         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8082          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:59000           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:2947                :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:7819            0.0.0.0:*
udp6       0      0 :::31267                :::*
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     79874    /var/run/docker/metrics.sock
unix  2      [ ACC ]     STREAM     LISTENING     72976    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     85583    @/containerd-shim/moby/
b01d94f718edd74477fb97a810671dd1021c55ba536ecccc5d0bbf2312c59973/shim.sock
unix  2      [ ACC ]     STREAM     LISTENING     79655    /var/run/docker/libnetwork/
f907179595ed.sock
unix  2      [ ACC ]     STREAM     [...]
```

3.5.2.2 Ensure IPv6 loopback traffic is configured

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).
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 (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Run the following commands to implement the loopback rules:
ip6tables -A INPUT -i lo -j ACCEPT # ip6tables -A OUTPUT -o lo -j ACCEPT # ip6tables -A INPUT -s ::1 -j DROP
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1S
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/ip6tables -L INPUT -v -n; /sbin/iptables -L OUTPUT -v -n' returned :

ip6tables v1.6.0:
can't initialize ip6tables table `filter': Permission denied (you must be root)


Perhaps ip6tables or your kernel needs to be upgraded.

iptables v1.6.0:
can't initialize iptables table `filter': Permission denied (you must be root)


Perhaps iptables or your kernel needs to be upgraded.
```

3.5.2.3 Ensure IPv6 outbound and established connections are configured

Info

Configure the firewall rules for new outbound, and established IPv6 connections.
Rationale:
If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2

QCSC-V1	6.2
QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The command '/sbin/ip6tables -L -v -n' returned :

ip6tables v1.6.0:
can't initialize ip6tables table `filter': Permission denied (you must be root)


Perhaps ip6tables or your kernel needs to be upgraded.
```

3.5.2.4 Ensure IPv6 firewall rules exist for all open ports

Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
Rationale:
Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:
ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
Notes:
Changing firewall settings while connected over network can result in being locked out of the system.
Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.
The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.13.1
800-53	SC-7(12)
CN-L3	8.1.10.6(j)
CSCV7	9.4
CSF	DE.CM-1
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.PT-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.13.1.3
ITSG-33	SC-7(12)
LEVEL	1NS
NESA	T4.5.4
NIAV2	AM38
NIAV2	SS13d
NIAV2	SS26
QCSC-V1	5.2.1
QCSC-V1	5.2.2
QCSC-V1	6.2

QCSC-V1	8.2.1
TBA-FIISB	43.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
 The command '/bin/netstat -ln; /sbin/ip6tables -L INPUT -v -n' returned :

ip6tables v1.6.0:
can't initialize ip6tables table `filter': Permission denied (you must be root)


Perhaps ip6tables or your kernel needs to be upgraded.
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:2947          0.0.0.0:*               LISTEN
tcp        0      0 172.31.8.1:6379         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8082          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:59000           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN
tcp6       0      0 ::1:2947                :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:7819            0.0.0.0:*
udp6       0      0 :::31267                :::*
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     79874    /var/run/docker/metrics.sock
unix  2      [ ACC ]     STREAM     LISTENING     72976    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     85583    @/containerd-shim/moby/
b01d94f718edd74477fb97a810671dd1021c55ba536ecccc5d0bbf2312c59973/shim.sock
unix  2      [ ACC ]     STREAM     LISTENING     79655    /var/run/docker/libnetwork/
f907179595ed.sock
unix  2      [ ACC ]     STREAM     [...]
```

4.3 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 unmanageable large.
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.
Notes:
If no maxage setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.

See Also

https://workbench.cisecurity.org/files/2619

References

800-53	AU-4
CSCV7	6.4
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	1NS
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

6.1.13 Audit SUID executables

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 program is to enable users to perform functions (such as changing their password) that require root privileges.
Rationale:
There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Ensure that no rogue SUID 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/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The following 22 files are SUID or SGID:

  /boot_device/p2/lower/bin/mount
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/mx-ver
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/ping
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/su
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/umount
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755

  /boot_device/p2/lower/usr/bin/bsd-write
     owner: root, group: tty, permissions: 2755

  /boot_device/p2/lower/usr/bin/chage
     owner: root, group: shadow, permissions: 2755
```

```
/boot_device/p2/lower/usr/bin/chfn
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/chsh
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/crontab
   owner: root, group: crontab, permissions: 2755

/boot_device/p2/lower/usr/bin/expiry
   owner: root, group: shadow, permissions: 2755

/boot_device/p2/lower/usr/bin/gpasswd
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/newgrp
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/passwd
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/ssh-agent
   owner: root, group: ssh, permissions: 2755

/boot_device/p2/lower/usr/bin/sudo
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/wall
   owner: root, group: tty, permissions: 2755

/boot_device/p2/lower/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   owner: root, group: messagebus, permissions: 4754

/boot_device/p2/lower/usr/lib/openssh/ssh-keysign
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/sbin/lldpcli
   owner: _lldpd, group: adm, permissions: 4750

/boot_device/p2/lower/usr/sbin/pppd
   owner: root, group: dip, permissions: 4754
```

6.1.14 Audit SGID executables

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 SGID program is to enable users to perform functions (such as changing their password) that require root privileges.
Rationale:
There are valid reasons for 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 md5 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 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/files/2619

References

800-171	3.4.2
800-53	CM-6
CSCV7	5.1
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
LEVEL	1NS
SWIFT-CSCV1	2.3

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The following 22 files are SUID or SGID:

  /boot_device/p2/lower/bin/mount
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/mx-ver
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/ping
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/su
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/bin/umount
     owner: root, group: root, permissions: 4755

  /boot_device/p2/lower/sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755

  /boot_device/p2/lower/usr/bin/bsd-write
     owner: root, group: tty, permissions: 2755

  /boot_device/p2/lower/usr/bin/chage
```

```
   owner: root, group: shadow, permissions: 2755

/boot_device/p2/lower/usr/bin/chfn
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/chsh
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/crontab
   owner: root, group: crontab, permissions: 2755

/boot_device/p2/lower/usr/bin/expiry
   owner: root, group: shadow, permissions: 2755

/boot_device/p2/lower/usr/bin/gpasswd
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/newgrp
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/passwd
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/ssh-agent
   owner: root, group: ssh, permissions: 2755

/boot_device/p2/lower/usr/bin/sudo
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/bin/wall
   owner: root, group: tty, permissions: 2755

/boot_device/p2/lower/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   owner: root, group: messagebus, permissions: 4754

/boot_device/p2/lower/usr/lib/openssh/ssh-keysign
   owner: root, group: root, permissions: 4755

/boot_device/p2/lower/usr/sbin/lldpcli
   owner: _lldpd, group: adm, permissions: 4750

/boot_device/p2/lower/usr/sbin/pppd
   owner: root, group: dip, permissions: 4754
```

6.2.3 Ensure no legacy '+' entries exist in /etc/shadow

Info

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.
Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

Solution

Remove any legacy '+' entries from /etc/shadow if they exist.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.5.1
800-53	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)
CSCV7	16.2
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-2
ITSG-33	IA-2a.
LEVEL	1S
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_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Info

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.
Rationale:
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.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

Solution

Making global modifications to user home directories 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 file permissions and determine the action to be taken in accordance with site policy.
Notes:
On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

See Also

https://workbench.cisecurity.org/files/2619

References

800-171	3.1.1
800-53	AC-3
CN-L3	8.1.4.2(f)
CN-L3	8.1.4.11(b)
CN-L3	8.1.10.2(c)
CN-L3	8.5.3.1
CN-L3	8.5.4.1(a)
CSCV6	3.1
CSCV7	14.6
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.4.1
ISO/IEC-27001	A.9.4.5
ITSG-33	AC-3
LEVEL	1S
NESA	T4.2.1
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	AM3
NIAV2	SS29
QCSC-V1	3.2
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	31.1

Audit File

CIS_Debian_Linux_9_Workstation_v1.0.1_L1.audit

Assets

security-aig-301.itest.conn.com

```
The following home directories have inappropriate permissions and/or ownership (mask:7027):

 /var/lib/snmp  mode: 0755 (should be 0750 or stricter) owner: Debian-snmp
 /var/run/lldpd  mode: 0755 (should be 0750 or stricter) owner: root
 /var/lib/aziot/edged  mode: 0755 (should be 0750 or stricter) owner: iotedge
 /var/run/dbus  mode: 0755 (should be 0750 or stricter) owner: root
 /var/lib/mosquitto  mode: 0755 (should be 0750 or stricter) owner: mosquitto
 /home/moxa  mode: 0755 (should be 0750 or stricter) owner: moxa
 /run/sshd  mode: 0755 (should be 0750 or stricter) owner: root
 /run/systemd  mode: 0755 (should be 0750 or stricter) owner: root
 /run/systemd/netif  mode: 0755 (should be 0750 or stricter) owner: systemd-network
 /run/systemd  mode: 0755 (should be 0750 or stricter) owner: root
 /var/lib/tpm  mode: 0755 (should be 0750 or stricter) owner: tss
```