172.26.99.119

Report generated by Nessus™ Wed, 02 Mar 2022 11:13:40 Sri Lanka Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

157118 (1) - CentOS 7 : httpd (CESA-2022:0143)

Synopsis

The remote CentOS Linux host is missing one or more security updates.

Description

The remote CentOS Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the CESA-2022:0143 advisory.

- httpd: mod_session: Heap overflow via a crafted SessionHeader value (CVE-2021-26691)

- httpd: NULL pointer dereference via malformed requests (CVE-2021-34798)

- httpd: Out-of-bounds write in ap_escape_quotes() via malicious input (CVE-2021-39275)

- httpd: mod_lua: Possible buffer overflow when parsing multipart content (CVE-2021-44790)

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://www.nessus.org/u?3c1968c4

https://cwe.mitre.org/data/definitions/119.html

https://cwe.mitre.org/data/definitions/400.html

https://cwe.mitre.org/data/definitions/476.html

https://cwe.mitre.org/data/definitions/787.html

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-26691
CVE	CVE-2021-34798
CVE	CVE-2021-39275
CVE	CVE-2021-44790
XREF	IAVA:2021-A-0259-S
XREF	IAVA:2021-A-0482
XREF	IAVA:2021-A-0440-S
XREF	IAVA:2021-A-0604
XREF	RHSA:2022:0143
XREF	CWE:119
XREF	CWE:400
XREF	CWE:476
XREF	CWE:787

Plugin Information

Published: 2022/01/26, Modified: 2022/01/26

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : httpd-2.4.6-97.el7.centos.2
Should be                : httpd-2.4.6-97.el7.centos.4

Remote package installed : httpd-tools-2.4.6-97.el7.centos.2
Should be                : httpd-tools-2.4.6-97.el7.centos.4
```

158439 (1) - CentOS 7 : cyrus-sasl (CESA-2022:0666)

Synopsis

The remote CentOS Linux host is missing a security update.

Description

The remote CentOS Linux 7 host has packages installed that are affected by a vulnerability as referenced in the CESA-2022:0666 advisory.

- cyrus-sasl: failure to properly escape SQL input allows an attacker to execute arbitrary SQL commands (CVE-2022-24407)

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://www.nessus.org/u?082201a6

https://cwe.mitre.org/data/definitions/20.html

https://cwe.mitre.org/data/definitions/89.html

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-24407
XREF	RHSA:2022:0666
XREF	CWE:20
XREF	CWE:89

Plugin Information

Published: 2022/02/25, Modified: 2022/02/25

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : cyrus-sasl-lib-2.1.26-23.el7
Should be                : cyrus-sasl-lib-2.1.26-24.el7_9
```

157138 (1) - CentOS 7 : polkit (CESA-2022:0274)

Synopsis

The remote CentOS Linux host is missing a security update.

Description

The remote CentOS Linux 7 host has packages installed that are affected by a vulnerability as referenced in the CESA-2022:0274 advisory.

- polkit: Local privilege escalation in pkexec due to incorrect handling of argument vector (CVE-2021-4034)

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://www.nessus.org/u?b3000b72

https://cwe.mitre.org/data/definitions/125.html

https://cwe.mitre.org/data/definitions/787.html

Solution

Update the affected polkit, polkit-devel and / or polkit-docs packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-4034
XREF	RHSA:2022:0274
XREF	IAVA:2022-A-0055
XREF	CWE:125
XREF	CWE:787

Plugin Information

Published: 2022/01/26, Modified: 2022/02/08

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : polkit-0.112-26.el7
Should be                : polkit-0.112-26.el7_9.1
```

158438 (1) - CentOS 7 : kernel (CESA-2022:0620)

Synopsis

The remote CentOS Linux host is missing one or more security updates.

Description

The remote CentOS Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the CESA-2022:0620 advisory.

- kernel: out of bounds write in hid-multitouch.c may lead to escalation of privilege (CVE-2020-0465)

- kernel: use after free in eventpoll.c may lead to escalation of privilege (CVE-2020-0466)

- kernel: Use After Free in unix_gc() which could result in a local privilege escalation (CVE-2021-0920)

- kernel: double free in bluetooth subsystem when the HCI device initialization fails (CVE-2021-3564)

- kernel: use-after-free in function hci_sock_bound_ioctl() (CVE-2021-3573)

- kernel: possible use-after-free in bluetooth module (CVE-2021-3752)

- kernel: xfs: raw block device data leak in XFS_IOC_ALLOCSP IOCTL (CVE-2021-4155)

- kernel: possible privileges escalation due to missing TLB flush (CVE-2022-0330)

- kernel: failing usercopy allows for use-after-free exploitation (CVE-2022-22942)

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://www.nessus.org/u?a13dc1ac

https://cwe.mitre.org/data/definitions/20.html

https://cwe.mitre.org/data/definitions/131.html

https://cwe.mitre.org/data/definitions/200.html

https://cwe.mitre.org/data/definitions/281.html

https://cwe.mitre.org/data/definitions/362.html

https://cwe.mitre.org/data/definitions/415.html

https://cwe.mitre.org/data/definitions/416.html

https://cwe.mitre.org/data/definitions/787.html

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-0465
CVE	CVE-2020-0466
CVE	CVE-2021-0920
CVE	CVE-2021-3564
CVE	CVE-2021-3573
CVE	CVE-2021-3752
CVE	CVE-2021-4155
CVE	CVE-2022-0330
CVE	CVE-2022-22942
XREF	RHSA:2022:0620
XREF	CWE:20
XREF	CWE:131
XREF	CWE:200
XREF	CWE:281
XREF	CWE:362
XREF	CWE:415
XREF	CWE:416
XREF	CWE:787

Plugin Information

Published: 2022/02/25, Modified: 2022/02/25

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : kernel-3.10.0-1160.49.1.el7
Should be                : kernel-3.10.0-1160.59.1.el7

Remote package installed : kernel-headers-3.10.0-1160.49.1.el7
Should be                : kernel-headers-3.10.0-1160.59.1.el7

Remote package installed : kernel-tools-3.10.0-1160.49.1.el7
Should be                : kernel-tools-3.10.0-1160.59.1.el7

Remote package installed : kernel-tools-libs-3.10.0-1160.49.1.el7
Should be                : kernel-tools-libs-3.10.0-1160.59.1.el7

Remote package installed : python-perf-3.10.0-1160.49.1.el7
Should be                : python-perf-3.10.0-1160.59.1.el7
```

158440 (1) - CentOS 7 : openldap (CESA-2022:0621)

Synopsis

The remote CentOS Linux host is missing one or more security updates.

Description

The remote CentOS Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the CESA-2022:0621 advisory.

- openldap: assertion failure in Certificate List syntax validation (CVE-2020-25709)

- openldap: assertion failure in CSN normalization with invalid input (CVE-2020-25710)

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://www.nessus.org/u?44b341b1

https://cwe.mitre.org/data/definitions/617.html

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-25709
CVE	CVE-2020-25710
XREF	RHSA:2022:0621
XREF	CWE:617

Plugin Information

Published: 2022/02/25, Modified: 2022/02/25

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : openldap-2.4.44-24.el7_9
Should be                : openldap-2.4.44-25.el7_9
```

11213 (1) - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604

BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

172.26.99.119 (tcp/80/www)

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus812813573.html HTTP/1.1
Connection: Close
Host: 172.26.99.119
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Wed, 02 Mar 2022 05:37:44 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus812813573.html HTTP/1.1
Connection: Keep-Alive
Host: 172.26.99.119
Pragma: no-cache
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

156820 (1) - CentOS 7 : kernel (CESA-2022:0063)

Synopsis

The remote CentOS Linux host is missing one or more security updates.

Description

The remote CentOS Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the CESA-2022:0063 advisory.

- kernel: perf_event_parse_addr_filter memory (CVE-2020-25704)

- kernel: fuse: fuse_do_getattr() calls make_bad_inode() in inappropriate situations (CVE-2020-36322)

- kernel: Heap buffer overflow in firedtv driver (CVE-2021-42739)

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://www.nessus.org/u?c56a1993

http://www.nessus.org/u?ae7a55d6

https://cwe.mitre.org/data/definitions/119.html

https://cwe.mitre.org/data/definitions/400.html

https://cwe.mitre.org/data/definitions/459.html

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-25704
CVE	CVE-2020-36322
CVE	CVE-2021-42739
XREF	RHSA:2022:0063
XREF	CWE:119
XREF	CWE:400
XREF	CWE:459

Plugin Information

Published: 2022/01/19, Modified: 2022/01/19

Plugin Output

172.26.99.119 (tcp/0)

```
Remote package installed : kernel-3.10.0-1160.49.1.el7
Should be                : kernel-3.10.0-1160.53.1.el7

Remote package installed : kernel-headers-3.10.0-1160.49.1.el7
Should be                : kernel-headers-3.10.0-1160.53.1.el7

Remote package installed : kernel-tools-3.10.0-1160.49.1.el7
Should be                : kernel-tools-3.10.0-1160.53.1.el7

Remote package installed : kernel-tools-libs-3.10.0-1160.49.1.el7
Should be                : kernel-tools-libs-3.10.0-1160.53.1.el7

Remote package installed : python-perf-3.10.0-1160.49.1.el7
Should be                : python-perf-3.10.0-1160.53.1.el7
```

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

172.26.99.119 (tcp/22/ssh)

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
```

```
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
```

153953 (1) - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

172.26.99.119 (tcp/22/ssh)

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

11219 (2) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/02/14

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

172.26.99.119 (tcp/80/www)

```
Port 80/tcp was found to be open
```

22964 (2) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

172.26.99.119 (tcp/80/www)

```
A web server is running on this port.
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

172.26.99.119 (tcp/80/www)

```
The remote web server type is :

Apache/2.4.6 (CentOS) PHP/5.4.16
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

172.26.99.119 (icmp/0)

```
The difference between the local and remote clocks is -28 seconds.
```

10267 (1) - 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.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/22/ssh)

```
SSH version : SSH-2.0-OpenSSH_7.4
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

172.26.99.119 (udp/0)

```
For your information, here is the traceroute from 172.26.75.228 to 172.26.99.119 :
172.26.75.228
172.26.75.225
172.26.90.69
172.26.99.119

Hop Count: 3
```

10881 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

  - 1.99
  - 2.0
```

11936 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/01/18

Plugin Output

172.26.99.119 (tcp/0)

```
Remote operating system : Linux Kernel 3.10.0-1160.49.1.el7.x86_64 on CentOS Linux release 7.9.2009
 (Core)
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_7.4
uname:Linux tspd-tnp360-web01-p 3.10.0-1160.49.1.el7.x86_64 #1 SMP Tue Nov 30 15:51:32 UTC 2021
 x86_64 x86_64 x86_64 GNU/Linux

SinFP:!:
   P1:B10113:F0x12:W29200:O0204ffff:M1460:
   P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190100_7_p=22R


The remote host is running Linux Kernel 3.10.0-1160.49.1.el7.x86_64 on CentOS Linux release 7.9.2009
 (Core)
```

18261 (1) - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2019/10/01

Plugin Output

172.26.99.119 (tcp/0)

```
The Linux distribution detected was :
 - CentOS 7
```

19506 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

172.26.99.119 (tcp/0)

```
Information about this scan :

Nessus version : 10.1.0
Nessus build : X20054
Plugin feed version : 202202271203
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
```

```
Scan name : 172.26.99.119
Scan policy used : Advanced Scan
Scanner IP : 172.26.75.228
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 37.878 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'svradmin' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2022/3/2 11:04 Sri Lanka Standard Time
Scan duration : 522 sec
```

20094 (1) - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

172.26.99.119 (tcp/0)

```
The remote host is a VMware virtual machine.
```

22869 (1) - 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.).

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

Plugin Information

Published: 2006/10/15, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/0)

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

  util-linux-2.23.2-65.el7_9.1|(none)
  libcgroup-0.41-21.el7|(none)
  grub2-tools-minimal-2.02-0.87.el7.centos.7|1
  libsemanage-python-2.5-14.el7|(none)
  NetworkManager-libnm-1.18.8-2.el7_9|1
  php-common-5.4.16-48.el7|(none)
  device-mapper-event-1.02.170-6.el7_9.5|7
  grub2-tools-2.02-0.87.el7.centos.7|1
  perl-Pod-Perldoc-3.20-4.el7|(none)
  authconfig-6.2.8-30.el7|(none)
  virt-what-1.18-4.el7_9.1|(none)
  perl-Pod-Usage-1.63-3.el7|(none)
  popt-1.13-16.el7|(none)
  NetworkManager-1.18.8-2.el7_9|1
  perl-Exporter-5.68-3.el7|(none)
  libattr-2.4.46-13.el7|(none)
  plymouth-0.8.9-0.34.20140113.el7.centos|(none)
  perl-Carp-1.26-244.el7|(none)
  kbd-legacy-1.15.5-16.el7_9|(none)
```

```
perl-File-Temp-0.23.01-3.el7|(none)
keyutils-libs-1.5.8-3.el7|(none)
NetworkManager-team-1.18.8-2.el7_9|1
perl-Filter-1.49-3.el7|(none)
libsysfs-2.1.0-16.el7|(none)
p11-kit-trust-0.23.5-3.el7|(none)
kexec-tools-2.0.15-51.el7_9.3|(none)
perl-Test-Harness-3.28-3.el7|(none)
ivtv-firmware-20080701-26.el7|2
openssh-clients-7.4p1-22.el7_9|(none)
pcre-devel-8.32-17.el7|(none)
httpd-2.4.6-97.el7.centos.2|(none)
automake-1.13.4-3.el7|(none)
gcc-4.8.5-44.el7|(none)
libmpc-1.0.1-3.el7|(none)
which-2.20-7.el7|(none)
libcroco-0.6.12-6.el7_9|(none)
gpg-pubkey-f4a80eb5-53a7ff4b|(none)
openssl-1.0.2k-22.el7_9|1
libICE-1.0.9-9.el7|(none)
python-kitchen-1.1.1-5.el7|(none)
findutils-4.5.11-6.el7|1
mesa-libGL-18.3.4-12.el7_9|(none)
urw-base35-fonts-common-20170801-10.el7|(none)
epel-release-7-14|(none)
lcms2-2.6-3.el7|(none)
iwl135-firmware-18.168.6.1-80.el7_9|(none)
libwayland-server-1.15.0-1.el7|(none)
libaio-0.3.109-13.el7|(none)
iwl100-firmware-39.31.5.1-80.el7_9|(none)
ilmbase-1.0.3-7.el7|(none)
cracklib-dicts-2.9.0-11.el7|(none)
iwl5000-firmware-8.83.5.1_1-80.el7_9|(none)
iwl4965-firmware-228.61.2.24-80.el7_9|(none)
jasper-devel-1.900.1-33.el7|(none)
libassuan-2.1.0-3.el7|(none)
fontconfig-2.13.0-4.3 [...]
```

24260 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

172.26.99.119 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

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

  Date: Wed, 02 Mar 2022 05:37:50 GMT
  Server: Apache/2.4.6 (CentOS) PHP/5.4.16
  X-Powered-By: PHP/5.4.16
  Content-Length: 1197
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html >
<head>
<meta charset="UTF-8">
<title>TNP 360&deg; - Log in</title>
<link rel="shortcut icon" href="Icons/AxiataLogoIco.ico"/>
<link rel="stylesheet" href="CSS/index.css">
```

```
  <script src="https://cdnjs.cloudflare.com/ajax/libs/prefixfree/1.0.7/prefixfree.min.js"></script>

</head>

<body>
  <div class="body"></div>
<div class="grad"></div>
<div class="logo">
<img src="Images/Logo7.png" style="width:auto;height:100px;" align="center">
</div>
<div class="header2">
<div><span><i>Digitizing Network Functions</i></span></div>
</div>
<br>
<form action="Controllers/Login.php" method="POST">
<form name="login">
<div class="login">
<input type="text" placeholder="Username" name="user" onfocus="if(this.value=='Username')
 this.value='';" onblur="if(this.value=='') this.value='Username';"><br>
<input type="password" placeholder="Password" name="password" onfocus="if(this.value=='Password')
 this.value='';" onblur="if(this.value=='') this.value='Password';"><br>
<input type="submit" onclick="check(this.form)" value="Log In" name="submit">
</div>
<script language="javascript">

function check(form)

</script>
</form>
</form>
```

25202 (1) - 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.

Solution

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

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2022/02/23

Plugin Output

172.26.99.119 (tcp/0)

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

 - ::1 (on interface lo)
 - fe80::250:56ff:fe87:12fa (on interface ens192)
```

25203 (1) - 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.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2022/02/23

Plugin Output

172.26.99.119 (tcp/0)

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

 - 127.0.0.1 (on interface lo)
 - 172.26.99.119 (on interface ens192)
```

25220 (1) - 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

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

172.26.99.119 (tcp/0)

33276 (1) - 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.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2018/08/13

Plugin Output

172.26.99.119 (tcp/0)

```
The following MAC address exists on the remote host :

  - 00:50:56:87:12:fa (interface ens192)
```

34098 (1) - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/0)

```
Version      : None
Vendor       : VMware, Inc.
Release Date : 12/12/2018
Secure boot  : disabled
```

35716 (1) - 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

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

172.26.99.119 (tcp/0)

```
The following card manufacturers were identified :

00:50:56:87:12:FA : VMware, Inc.
```

39520 (1) - 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

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

39521 (1) - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

172.26.99.119 (tcp/80/www)

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

45590 (1) - 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

Plugin Information

Published: 2010/04/21, Modified: 2022/02/14

Plugin Output

172.26.99.119 (tcp/0)

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

  cpe:/o:centos:centos:7:update9 -> CentOS

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.6 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:gnupg:libgcrypt:1.5.3 -> GnuPG Libgcrypt
  cpe:/a:mariadb:mariadb:5.5.68 -> MariaDB for Node.js
  cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.4.16 -> PHP PHP
```

48204 (1) - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/80/www)

```
URL        : http://172.26.99.119/
Version    : 2.4.6
backported : 1
modules    : PHP/5.4.16
os         : ConvertedCentOS
```

48243 (1) - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/80/www)

```
Nessus was able to identify the following PHP version information :

  Version : 5.4.16
  Source  : Server: Apache/2.4.6 (CentOS) PHP/5.4.16
  Source  : X-Powered-By: PHP/5.4.16
```

54615 (1) - 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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

172.26.99.119 (tcp/0)

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

55472 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2022/02/23

Plugin Output

172.26.99.119 (tcp/0)

```
Hostname : tspd-tnp360-web01-p
  tspd-tnp360-web01-p (hostname command)
```

56468 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

172.26.99.119 (tcp/0)

```
The host has not yet been rebooted.
```

66334 (1) - 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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2022/02/14

Plugin Output

172.26.99.119 (tcp/0)

```
. You need to take the following 5 actions :

[ CentOS 7 : cyrus-sasl (CESA-2022:0666) (158439) ]

+ Action to take : Update the affected packages.

[ CentOS 7 : httpd (CESA-2022:0143) (157118) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ CentOS 7 : kernel (CESA-2022:0620) (158438) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 12 different vulnerabilities (CVEs).


[ CentOS 7 : openldap (CESA-2022:0621) (158440) ]

+ Action to take : Update the affected packages.
```

```
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ CentOS 7 : polkit (CESA-2022:0274) (157138) ]

+ Action to take : Update the affected polkit, polkit-devel and / or polkit-docs packages.
```

70657 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

172.26.99.119 (tcp/22/ssh)

```
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-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  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 :

  3des-cbc
```

```
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  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_ [...]
```

84574 (1) - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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

Plugin Information

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

172.26.99.119 (tcp/80/www)

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

86420 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

172.26.99.119 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 00:50:56:87:12:FA
```

90707 (1) - 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

Plugin Information

Published: 2016/04/26, Modified: 2017/08/28

Plugin Output

172.26.99.119 (tcp/22/ssh)

95928 (1) - 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.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2019/04/04

Plugin Output

172.26.99.119 (tcp/0)

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

User         : neutron
Home folder  : /home/neutron
Start script : /bin/bash
Groups       : neutron

User         : svradmin
Home folder  : /home/svradmin
Start script : /bin/bash
Groups       : svradmin
               apache

User         : apache
Home folder  : /usr/share/httpd
Start script : /sbin/nologin
Groups       : apache

User         : sysauto
Home folder  : /home/sysauto
Start script : /bin/bash
Groups       : sysauto

User         : awsmra
Home folder  : /home/awsmra
Start script : /bin/bash
Groups       : awsmra
```

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

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

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

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

User         : adm
Home folder  : /var/adm
Start script : /sbin/nologin
Groups       : adm

User         : lp
Home folder  : /var/spool/lpd
Start script : /sbin/nologin
Groups       : lp

User         : sync
Home folder  : /sbin
Start script : /sbin/nologin
Groups       : root

User         : shutdown
Home folder  : /sbin
Start script : /sbin/nologin
Groups       : root

User         : halt
Home folder  : /sbin
Start script : /sbin/nologin
Groups       : root

User         : mail
Home folder  : /var/spool/mail
Start script : /sbin/nologin
Groups       : mail

User         : operator
Home folder  : /root
Start script : /sbin/nologin
Groups       : root

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

User         : ftp
Home folder  : /var/ftp
Start script : /sbin/nologin
Groups       : ftp

User         : nobody
Home folder  : /
Start script : /sbin/nologin
Groups       : nobody

User         : systemd-network
Home folder  : /
Start script : /sbin/nologin
```

```
Groups       : systemd-network

User         : dbus
Home folder  : /
Start script : /sbin/nologin
Groups       : dbus

User         : polkitd
Home  [...]
```

97993 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2021/08/02

Plugin Output

172.26.99.119 (tcp/0)

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

The output of "uname -a" is :
Linux tspd-tnp360-web01-p 3.10.0-1160.49.1.el7.x86_64 #1 SMP Tue Nov 30 15:51:32 UTC 2021 x86_64
 x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote CentOS system is :
CentOS Linux release 7.9.2009 (Core)

OS Security Patch Assessment is available for this host.
Runtime : 8.648823 seconds
```

102094 (1) - 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'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

172.26.99.119 (tcp/0)

```
Login account : svradmin
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/cache/httpd 2>&1"
      Response : "grep: /var/cache/httpd: Permission denied"
      Error    : ""
    - Command  : "grep -aE '.*(Apache\\/([0-9][0-9]?\\.[0-9][0-9]?\\.[0-9][0-9]?) \\([A-Za-z ]+\
\)).*' /var/cache/httpd 2>&1"
      Response : "grep: /var/cache/httpd: Permission denied"
      Error    : ""
```

```
    - Command  : "grep -aE '(Oracle-HTTP-Server)' /var/log/httpd 2>&1"
      Response : "grep: /var/log/httpd: Permission denied"
      Error    : ""
    - Command  : "grep -aE '.*(Apache\\/([0-9][0-9]?\\.[0-9][0-9]?\\.[0-9][0-9]?) \\([A-Za-z ]+\
\)).*' /var/log/httpd 2>&1"
      Response : "grep: /var/log/httpd: Permission denied"
      Error    : ""
    - Command  : "grep -aE '(Oracle-HTTP-Server)' /var/run/httpd 2>&1"
      Response : "grep: /var/run/httpd: Permission denied"
      Error    : ""
    - Command  : "grep -aE '.*(Apache\\/([0-9][0-9]?\\.[0-9][0-9]?\\.[0-9][0-9]?) \\([A-Za-z ]+\
\)).*' /var/run/httpd 2>&1"
      Response : "grep: /var/run/httpd: Permission denied"
      Error    : ""
  - Plugin Filename : bios_get_info_ssh.nasl
    Plugin ID       : 34098
    Plugin Name     : BIOS Info (SSH)
    - Command  : "LC_ALL=C /usr/sbin/dmidecode"
      Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\n/dev/mem:
 Permission denied"
    - Command  : "LC_ALL=C /sbin/dmidecode"
      Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\n/dev/mem:
 Permission denied"
  - Plugin Filename : enumerate_oci_nix.nasl
    Plugin ID       : 154138
    Plugin Name     : Oracle Cloud In [...]
```

110385 (1) - 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.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2021/07/26

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

User:       'svradmin'
Port:       22
Proto:      SSH
Method:     password
Escalation: Nothing


See the output of the following plugin for details :

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

110483 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2021/02/04

Plugin Output

172.26.99.119 (tcp/0)

```
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.1 128116  6764 ?        Ss    2021   8:33 /usr/lib/systemd/systemd --
switched-root --system --deserialize 22
root          2  0.0  0.0      0     0 ?        S     2021   0:01 [kthreadd]
root          4  0.0  0.0      0     0 ?        S<    2021   0:00 [kworker/0:0H]
root          6  0.0  0.0      0     0 ?        S     2021   0:03 [ksoftirqd/0]
root          7  0.0  0.0      0     0 ?        S     2021   0:01 [migration/0]
root          8  0.0  0.0      0     0 ?        S     2021   0:00 [rcu_bh]
root          9  0.0  0.0      0     0 ?        S     2021   4:57 [rcu_sched]
root         10  0.0  0.0      0     0 ?        S<    2021   0:00 [lru-add-drain]
root         11  0.0  0.0      0     0 ?        S     2021   0:34 [watchdog/0]
root         12  0.0  0.0      0     0 ?        S     2021   0:49 [watchdog/1]
root         13  0.0  0.0      0     0 ?        S     2021   0:01 [migration/1]
root         14  0.0  0.0      0     0 ?        S     2021   0:26 [ksoftirqd/1]
root         16  0.0  0.0      0     0 ?        S<    2021   0:00 [kworker/1:0H]
root         18  0.0  0.0      0     0 ?        S     2021   0:00 [kdevtmpfs]
root         19  0.0  0.0      0     0 ?        S<    2021   0:00 [netns]
root         20  0.0  0.0      0     0 ?        S     2021   0:08 [khungtaskd]
root         21  0.0  0.0      0     0 ?        S<    2021   0:00 [writeback]
root         22  0.0  0.0      0     0 ?        S<    2021   0:00 [kintegrityd]
root         23  0.0  0.0      0     0 ?        S<    2021   0:00 [bioset]
root         24  0.0  0.0      0     0 ?        S<    2021   0:00 [bioset]
root         25  0.0  0.0      0     0 ?        S<    2021   0:00 [bioset]
root         26  0.0  0.0      0     0 ?        S<    2021   0:00 [kblockd]
root         27  0.0  0.0      0     0 ?        S<    2021   0:00 [md]
root         28  0.0  0.0      0     0 ?        S<    2021   0:00 [edac-poller]
root         29  0.0  0.0      0     0 ?        S<    2021   0:00 [watchdog [...]
```

117887 (1) - 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.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

172.26.99.119 (tcp/0)

```
OS Security Patch Assessment is available.

Account  : svradmin
Protocol : SSH
```

130626 (1) - MariaDB Client/Server Installed (Linux)

Synopsis

One or more MariaDB server or client versions are available on the remote Linux host.

Description

One or more MariaDB server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/08, Modified: 2022/02/14

Plugin Output

172.26.99.119 (tcp/0)

```
Path    : mariadb (via package manager)
Version : 5.5.68
Product : MariaDB Server
```

141118 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2021/07/26

Plugin Output

172.26.99.119 (tcp/22/ssh)

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

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

```
Escalation: Nothing
```

141394 (1) - 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

Plugin Information

Published: 2020/10/12, Modified: 2022/02/24

Plugin Output

172.26.99.119 (tcp/0)

```
Path               : /usr/sbin/httpd
Version            : 2.4.6
Associated Package : httpd-2.4.6-97.el7.centos.2.x86_64
Managed by OS      : True
Running            : yes

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

Loaded modules :
  - libphp5
  - mod_access_compat
  - mod_actions
  - mod_alias
  - mod_allowmethods
  - mod_auth_basic
  - mod_auth_digest
```

```
    - mod_authn_anon
    - mod_authn_core
    - mod_authn_dbd
    - mod_authn_dbm
    - mod_authn_file
    - mod_authn_socache
    - mod_authz_core
    - mod_authz_dbd
    - mod_authz_dbm
    - mod_authz_groupfile
    - mod_authz_host
    - mod_authz_owner
    - mod_authz_user
    - mod_autoindex
    - mod_cache
    - mod_cache_disk
    - mod_cgi
    - mod_cgid
    - mod_cgid
    - mod_data
    - mod_dav
    - mod_dav_fs
    - mod_dav_lock
    - mod_dbd
    - mod_deflate
    - mod_dir
    - mod_dumpio
    - mod_echo
    - mod_env
    - mod_expires
    - mod_ext_filter
    - mod_filter
    - mod_headers
    - mod_include
    - mod_info
    - mod_lbmethod_bybusyness
    - mod_lbmethod_byrequests
    - mod_lbmethod_bytraffic
    - mod_lbmethod_heartbeat
    - mod_log_config
    - mod_logio
    - mod_lua
    - mod_mime
    - mod_mime_magic
    - mod_mpm_prefork
    - mod_negotiation
    - mod_proxy
    - mod_proxy_ajp
    - mod_proxy_balancer
    - mod_proxy_connect
    - mod_proxy_express
    - mod_proxy_fcgi
    - mod_proxy_fdpass
    - mod_proxy_ftp
    - mod_proxy_http
    - mod_proxy_scgi
    - mod_proxy_wstunnel
    - mod_remoteip
    - mod_reqtimeout
    - mod_rewrite
    - mod_setenvif
    - mod_slotmem_plain
    - mod_slotmem_shm
    - mod_socache_dbm
    - mod_socache_memcache
    - mod_socache_shmcb
    - mod_status
    - mod_substitute
    - mod_suexec
    - mod_systemd
```

```
      - mod_unique_id
      - mod_unixd
      - mod_userdir
      - mod_version
      - mod_vhost_alias
```

149334 (1) - 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

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

172.26.99.119 (tcp/22/ssh)

151883 (1) - 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

Plugin Information

Published: 2021/07/21, Modified: 2022/02/24

Plugin Output

172.26.99.119 (tcp/0)

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /usr/lib64/libgcrypt.so.11.8.2
  Version : 1.5.3

  Path    : /usr/lib64/libgcrypt.so.11
  Version : 1.5.3
```

152743 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

172.26.99.119 (tcp/0)

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

  unzip -v                    :
    bash: unzip: command not found


Account  : svradmin
```

```
Protocol : SSH
```

153588 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2021/09/23

Plugin Output

172.26.99.119 (tcp/22/ssh)

```
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
```