Lab 11 – Peck

Report generated by Nessus™ Fri, 11 Nov 2022 14:56:29 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

3.232.117.195

0	11	1	2	44
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Nov 11 14:53:18 2022
End time:	Fri Nov 11 14:56:29 2022

Host Information

IP:	3.232.117.195
MAC Address:	0E:D9:FD:35:1A:8D
OS:	Linux Kernel 3.10.0-1160.15.2.el7.x86_64 on CentOS Linux release 7.9.2009 (Core)

Vulnerabilities

147885 - CentOS 7 : kernel (CESA-2021:0856)

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-2021:0856 advisory.

- kernel: malicious USB devices can lead to multiple out-of-bounds write (CVE-2019-19532)

- kernel: out-of-bounds reads in pinctrl subsystem. (CVE-2020-0427)

- kernel: performance counters race condition use-after-free (CVE-2020-14351)

- kernel: Local buffer overflow in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c (CVE-2020-25211)

- kernel: Geneve/IPsec traffic may be unencrypted between two Geneve endpoints (CVE-2020-25645)

- kernel: use-after-free in read in vt_do_kdgkb_ioctl (CVE-2020-25656)

- kernel: ICMP rate limiting can be used for DNS poisoning attack (CVE-2020-25705)

- kernel: SCSI target (LIO) write to any block on ILO backstore (CVE-2020-28374)

- kernel: locking issue in drivers/tty/tty_jobctrl.c can lead to an use-after-free (CVE-2020-29661)

- kernel: use-after-free in i915_ppgtt_close in drivers/gpu/drm/i915/i915_gem_gtt.c (CVE-2020-7053)

- kernel: increase slab leak leads to DoS (CVE-2021-20265)

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?7bf93600

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

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

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

https://cwe.mitre.org/data/definitions/319.html

https://cwe.mitre.org/data/definitions/330.html

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

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

https://cwe.mitre.org/data/definitions/667.html

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/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

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-19532
CVE	CVE-2020-0427

CVE	CVE-2020-7053
CVE	CVE-2020-14351
CVE	CVE-2020-25211
CVE	CVE-2020-25645
CVE	CVE-2020-25656
CVE	CVE-2020-25705
CVE	CVE-2020-28374
CVE	CVE-2020-29661
CVE	CVE-2021-20265
XREF	RHSA:2021:0856
XREF	CWE:20
XREF	CWE:119
XREF	CWE:200
XREF	CWE:319
XREF	CWE:330
XREF	CWE:400
XREF	CWE:416
XREF	CWE:667

Plugin Information

Published: 2021/03/18, Modified: 2022/05/10

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.21.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.21.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.21.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

148425 - CentOS 7 : kernel (CESA-2021:1071)

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-2021:1071 advisory.

- kernel: iscsi: unrestricted access to sessions and handles (CVE-2021-27363)

- kernel: out-of-bounds read in libiscsi module (CVE-2021-27364)

- kernel: heap buffer overflow in the iSCSI subsystem (CVE-2021-27365)

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?a94c4338

https://cwe.mitre.org/data/definitions/122.html

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

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

https://cwe.mitre.org/data/definitions/250.html

Solution

Update the affected packages.

Risk Factor

Medium

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

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-2021-27363
CVE	CVE-2021-27364
CVE	CVE-2021-27365
XREF	RHSA:2021:1071
XREF	CWE:122
XREF	CWE:125
XREF	CWE:200
XREF	CWE:250

Plugin Information

Published: 2021/04/10, Modified: 2021/04/10

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.24.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.24.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.24.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

150770 - CentOS 7 : kernel (CESA-2021:2314)

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-2021:2314 advisory.

- kernel: Integer overflow in Intel(R) Graphics Drivers (CVE-2020-12362)

- kernel: Improper input validation in some Intel(R) Graphics Drivers (CVE-2020-12363)

- kernel: Null pointer dereference in some Intel(R) Graphics Drivers (CVE-2020-12364)

- kernel: Speculation on pointer arithmetic against bpf_context pointer (CVE-2020-27170)

- kernel: use-after-free in n_tty_receive_buf_common function in drivers/tty/n_tty.c (CVE-2020-8648)

- kernel: Use after free via PI futex state (CVE-2021-3347)

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?38256049

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

https://cwe.mitre.org/data/definitions/190.html

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

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

https://cwe.mitre.org/data/definitions/476.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-2020-8648
CVE	CVE-2020-12362
CVE	CVE-2020-12363
CVE	CVE-2020-12364
CVE	CVE-2020-27170
CVE	CVE-2021-3347
XREF	RHSA:2021:2314
XREF	CWE:20
XREF	CWE:190
XREF	CWE:200
XREF	CWE:416
XREF	CWE:476

Plugin Information

Published: 2021/06/14, Modified: 2021/06/14

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.31.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.31.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.31.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

151979 - CentOS 7 : kernel (CESA-2021:2725)

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-2021:2725 advisory.

- kernel: use-after-free in show_numa_stats function (CVE-2019-20934)

- kernel: mishandles invalid descriptors in drivers/media/usb/gspca/xirlink_cit.c (CVE-2020-11668)

- kernel: use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c (CVE-2021-33033)

- kernel: use-after-free in net/bluetooth/hci_event.c when destroying an hci_chan (CVE-2021-33034)

- kernel: size_t-to-int conversion vulnerability in the filesystem layer (CVE-2021-33909)

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?53b63f94

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

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

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

II

References

CVE	CVE-2019-20934
CVE	CVE-2020-11668
CVE	CVE-2021-33033
CVE	CVE-2021-33034
CVE	CVE-2021-33909
XREF	RHSA:2021:2725
XREF	IAVA:2021-A-0350
XREF	CWE:20
XREF	CWE:416
XREF	CWE:476
XREF	CWE:787

Plugin Information

Published: 2021/07/22, Modified: 2021/07/30

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.36.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.36.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.36.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

152970 - CentOS 7 : kernel (CESA-2021:3327)

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-2021:3327 advisory.

- kernel: powerpc: RTAS calls can be used to compromise kernel integrity (CVE-2020-27777)

- kernel: out-of-bounds write in xt_compat_target_from_user() in net/netfilter/x_tables.c (CVE-2021-22555)

- kernel: Local privilege escalation due to incorrect BPF JIT branch displacement computation (CVE-2021-29154)

- kernel: lack a full memory barrier upon the assignment of a new table value in net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h may lead to DoS (CVE-2021-29650)

- kernel: race condition for removal of the HCI controller (CVE-2021-32399)

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?f7c44f94

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

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

https://cwe.mitre.org/data/definitions/662.html

https://cwe.mitre.org/data/definitions/667.html

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

https://cwe.mitre.org/data/definitions/862.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

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)

References

CVE	CVE-2020-27777
CVE	CVE-2021-22555
CVE	CVE-2021-29154
CVE	CVE-2021-29650
CVE	CVE-2021-32399
XREF	RHSA:2021:3327
XREF	CWE:119
XREF	CWE:362
XREF	CWE:662
XREF	CWE:667
XREF	CWE:787
XREF	CWE:862

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2021/09/02, Modified: 2022/08/31

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.41.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.41.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.41.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

153767 - CentOS 7 : kernel (CESA-2021:3438)

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-2021:3438 advisory.

- kernel: use-after-free in route4_change() in net/sched/cls_route.c (CVE-2021-3715)

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?74230ed2

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

https://access.redhat.com/security/cve/cve-2021-3715

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-2021-3715
XREF	RHSA:2021:3438
XREF	CWE:416

Plugin Information

Published: 2021/09/27, Modified: 2022/03/11

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.42.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.42.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.42.2.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

155547 - CentOS 7 : kernel (CESA-2021:3801)

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-2021:3801 advisory.

- kernel: Improper handling of VM_IO|VM_PFNMAP vmas in KVM can bypass RO checks (CVE-2021-22543)

- kernel: SVM nested virtualization issue in KVM (AVIC support) (CVE-2021-3653)

- kernel: SVM nested virtualization issue in KVM (VMLOAD/VMSAVE) (CVE-2021-3656)

- kernel: powerpc: KVM guest OS users can cause host OS memory corruption (CVE-2021-37576)

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?a2d7e1e5

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

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

https://cwe.mitre.org/data/definitions/862.html

https://cwe.mitre.org/data/definitions/863.html

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (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-2021-3653
CVE	CVE-2021-3656
CVE	CVE-2021-22543
CVE	CVE-2021-37576
XREF	RHSA:2021:3801
XREF	CWE:20
XREF	CWE:119
XREF	CWE:862
XREF	CWE:863

Plugin Information

Published: 2021/11/17, Modified: 2022/05/06

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.45.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.45.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.45.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

155759 - CentOS 7 : kernel (CESA-2021:4777)

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-2021:4777 advisory.

- kernel: use-after-free in drivers/infiniband/core/ucma.c ctx use-after-free (CVE-2020-36385)

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?90a2cef0

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

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-36385
XREF	RHSA:2021:4777

XREF	CWE:416

Plugin Information

Published: 2021/12/01, Modified: 2021/12/01

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.49.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.49.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.49.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

158438 - 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

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

CVSS v2.0 Base Score

7.9 (CVSS2#AV:A/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.9 (CVSS2#E:H/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	CISA-KNOWN-EXPLOITED:2022/06/13
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: 2022/05/25

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.59.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.59.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.59.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

161374 - CentOS 7 : kernel (CESA-2022:4642)

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-2022:4642 advisory.

- kernel: cgroups v1 release_agent feature may allow privilege escalation (CVE-2022-0492)

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?cbe41c13

Solution

Update the affected packages.

Risk Factor

Medium

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0492
XREF	RHSA:2022:4642
XREF	CWE:287

Plugin Information

Published: 2022/05/19, Modified: 2022/10/20

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.66.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.66.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.66.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

163735 - CentOS 7 : kernel (CESA-2022:5232)

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-2022:5232 advisory.

- kernel: race condition in perf_event_open leads to privilege escalation (CVE-2022-1729)

- kernel: a use-after-free write in the netfilter subsystem can lead to privilege escalation to root (CVE-2022-1966)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?546ed734

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-2022-1729

CVE	CVE-2022-1966
XREF	RHSA:2022:5232
XREF	CWE:362
XREF	CWE:416

Plugin Information

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

Plugin Output

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.71.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.71.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.71.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

156820 - 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

tcp/0

```
Installed package kernel-3.10.0-1160.76.1.el7 is greater than kernel-3.10.0-1160.53.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-3.10.0-1160.76.1.el7 is greater than kernel-
tools-3.10.0-1160.53.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.

Installed package kernel-tools-libs-3.10.0-1160.76.1.el7 is greater than kernel-tools-
libs-3.10.0-1160.53.1.el7.
However, according to uname -r, the current running kernel level is 3.10.0-1160.15.2.el7.
This system requires a reboot to begin using the patched kernel level.
```

70658 - 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

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 - 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

tcp/22/ssh

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

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

90191 - Amazon Web Services EC2 Instance Metadata Enumeration (Unix)

Synopsis

The remote host is an AWS EC2 instance for which metadata could be retrieved.

Description

The remote host appears to be an Amazon Machine Image. Nessus was able to use the metadata API to collect information about the system.

See Also

https://docs.aws.amazon.com/ec2/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/03/25, Modified: 2022/11/07

Plugin Output

tcp/0

```

It was possible to retrieve the following API items :

  - accountId: 628630791266
  - architecture: x86_64
  - availabilityZone: us-east-1a
  - billingProducts: null
  - devpayProductCodes: null
  - marketplaceProductCodes: null
  - imageId: ami-04cafed56c23f83aa
  - instanceId: i-0cd7e2b6dbfc712c9
  - instanceType: t2.nano
  - kernelId: null
  - pendingTime: 2022-11-05T01:05:05Z
  - privateIp: 172.26.12.151
  - ramdiskId: null
  - region: us-east-1
  - version: 2017-09-30
  - instance-id: i-0cd7e2b6dbfc712c9
  - public-hostname: ec2-3-232-117-195.compute-1.amazonaws.com
  - hostname: ip-172-26-12-151.ec2.internal
  - local-ipv4: 172.26.12.151
  - local-hostname: ip-172-26-12-151.ec2.internal
  - public-ipv4: 3.232.117.195
```

```
      - ami-id: ami-04cafed56c23f83aa
      - mac: 0e:d9:fd:35:1a:8d
      - block-device-mapping-ami: /dev/sda1
      - block-device-mapping-root: /dev/sda1
      - block-device-mapping-ebs-count: 0
      - block-device-mapping-ephemeral-count: 0
      - vpc-id: vpc-0e02d94842bc5e204
```

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

Plugin Information

Published: 2020/10/12, Modified: 2022/10/05

Plugin Output

tcp/0

```
Path               : /usr/sbin/httpd
Version            : 2.4.6
Associated Package : httpd-2.4.6-97.el7.centos.5.x86_64
Managed by OS      : True
Running            : no

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

Loaded modules :
  - 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_ssl
      - mod_status
      - mod_substitute
      - mod_suexec
      - mod_systemd
      - mod_unique_id
      - mod_unixd
      - mod_userdir
      - mod_version
      - mod_vhost_alias
```

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

Plugin Information

Published: 2020/11/09, Modified: 2022/10/05

Plugin Output

tcp/0

```
Sites and configs present in /usr/sbin/httpd Apache installation:
  - following sites are present in /etc/httpd/conf/httpd.conf Apache config file:
    +   - *:443
```

34098 - 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: 2022/06/29

Plugin Output

tcp/0

```
Version      : 4.11.amazon
Vendor       : Xen
Release Date : 08/24/2006
UUID         : ec20d514-b773-ba11-2e6c-f24259fd10e6
Secure boot  : disabled
```

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

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

Plugin Information

Published: 2010/04/21, Modified: 2022/10/05

Plugin Output

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:openbsd:openssh:7.4 -> OpenBSD OpenSSH
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2022/10/11

Plugin Output

tcp/0

```
Hostname : ip-172-26-12-151.ec2.internal
  ip-172-26-12-151.ec2.internal (hostname command)
```

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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

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

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.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```

The following IPv4 addresses are set on the remote host :

 - 172.26.12.151 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

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.

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

tcp/0

```

The following IPv6 interfaces are set on the remote host :

 - fe80::cd9:fdff:fe35:1a8d (on interface eth0)
 - 2600:1f18:6180:8000:89f:2b50:378f:4005 (on interface eth0)
 - ::1 (on interface lo)
```

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.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

  - 0e:d9:fd:35:1a:8d (interface eth0)
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 0E:D9:FD:35:1A:8D
```

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

Plugin Information

Published: 2021/07/21, Modified: 2022/10/06

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

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

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

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2022/09/08

Plugin Output

tcp/0

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        219M     0  219M   0% /dev
tmpfs           243M     0  243M   0% /dev/shm
tmpfs           243M   33M  211M  14% /run
tmpfs           243M     0  243M   0% /sys/fs/cgroup
/dev/xvda1       20G  2.4G   18G  12% /
tmpfs            49M     0   49M   0% /run/user/1000


$ lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  20G  0 disk 
`-xvda1 202:1    0  20G  0 part /


$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=224172k,nr_inodes=56043,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,seclabel,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,seclabel,mode=755)
```

```
cgroup on /sys/fs/cgroup/systemd type cgroup
 (rw,nosuid,nodev,noexec,relatime,seclabel,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-
agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,cpuset)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup
 (rw,nosuid,nodev,noexec,relatime,seclabel,net_prio,net_cls)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,freezer)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup
 (rw,nosuid,nodev,noexec,relatime,seclabel,cpuacct,cpu)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,seclabel,hugetlb)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec [...]
```

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.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2022/06/29

Plugin Output

tcp/0

```

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

User         : centos
Home folder  : /home/centos
Start script : /bin/bash
Groups       : centos
               systemd-journal
               adm

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

User         : tss
Home folder  : /dev/null
Start script : /sbin/nologin
Groups       : tss

----------[ 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 : /bin/sync
Groups       : root

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

User         : halt
Home folder  : /sbin
Start script : /sbin/halt
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 folder  : /
Start script : /sbin/nologin
```

```
Groups       : polkitd

User         : rpc
Home folder  : /var/lib/rpcbind
Start script : /sbin/nologin
Groups       : rpc

User         : rpcuser
Hom [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2022/06/09

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.4.1
Nessus build : 20091
Plugin feed version : 202211111345
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : es8-x86-64
Scan type : Normal
Scan name : Lab 11 - Peck
Scan policy used : Basic Network Scan
Scanner IP : 172.20.0.2
Port scanner(s) : netstat
Port range : default
Ping RTT : 21.347 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'centos' 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 : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2022/11/11 14:53 UTC
Scan duration : 169 sec
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2021/09/16

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

tcp/22/ssh

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

tcp/111

```
Port 111/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

udp/111

```
Port 111/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

udp/546

```
Port 546/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2022/07/11

Plugin Output

udp/717

```
Port 717/udp 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.10.0-1160.15.2.el7.x86_64 on CentOS Linux release 7.9.2009
 (Core)
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.10.0-1160.15.2.el7.x86_64 on CentOS Linux release 7.9.2009
 (Core)
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```

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

The output of "uname -a" is :
Linux ip-172-26-12-151.ec2.internal 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 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 : 7.588586 seconds
```

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.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

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

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account  : centos
Protocol : SSH
```

154138 - Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)

Synopsis

The remote host is an OCI (Oracle Cloud Infrastructure) instance for which metadata could be retrieved.

Description

The remote host is an OCI (Oracle Cloud Infrastructure) instance for which metadata could be retrieved.

See Also

https://www.oracle.com/ie/cloud/compute/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/10/14, Modified: 2022/06/29

Plugin Output

tcp/0

```
The following items could not be retrieved :

  - instance
  - vnics
  - volumeAttachments
```

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2022/11/08

Plugin Output

tcp/0

```

. You need to take the following action :

[ CentOS 7 : kernel (CESA-2022:5232) (163735) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 49 different vulnerabilities (CVEs).

```

133964 - SELinux Status Check

Synopsis

SELinux is available on the host and plugin was able to check if it is enabled.

Description

SELinux is available on the host and plugin was able to check if it is enabled.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/02/25, Modified: 2022/10/05

Plugin Output

tcp/0

```
SELinux config has been found on the host.

SELinux is enabled.
SELinux policy: targeted.
SELinux status: enforcing.
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

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_ [...]
```

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'.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0507

Plugin Information

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

Plugin Output

tcp/0

```
Login account : centos
Commands failed due to privilege escalation failure:
- Escalation account : centos
  Escalation method  : sudo
  Plugins :
  - Plugin Filename : apache_http_server_nix_installed.nbin
    Plugin ID       : 141394
    Plugin Name     : Apache HTTP Server Installed (Linux)
    - Command  : "strings '/var/run/httpd' 2>&1"
      Response : "strings: /var/run/httpd: Permission denied"
      Error    : ""
    - Command  : "strings '/var/run/httpd' 2>&1"
      Response : "strings: /var/run/httpd: Permission denied"
      Error    : ""
    - Command  : "strings '/var/log/httpd' 2>&1"
      Response : "strings: /var/log/httpd: Permission denied"
      Error    : ""
    - Command  : "strings '/var/log/httpd' 2>&1"
      Response : "strings: /var/log/httpd: Permission denied"
      Error    : ""
    - Command  : "strings '/var/cache/httpd' 2>&1"
      Response : "strings: /var/cache/httpd: Permission denied"
      Error    : ""
    - Command  : "strings '/var/cache/httpd' 2>&1"
      Response : "strings: /var/cache/httpd: Permission denied"
      Error    : ""
  - Plugin Filename : bios_get_info_ssh.nasl
    Plugin ID       : 34098
    Plugin Name     : BIOS Info (SSH)
    - Command  : "LC_ALL=C dmidecode"
      Response : "# dmidecode 3.2\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\n/dev/mem: Permission denied"
      Error    : ""
    - Command  : "LC_ALL=C /usr/sbin/dmidecode"
      Response : "# dmidecode 3.2\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\n/dev/mem: Permission denied"
      Error    : ""
    - Command  : "LC_ALL=C /sbin/dmidecode"
      Response : "# dmidecode 3.2\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied
\nScanning /dev/mem for entry point.\n/dev/mem: Permission denied"
      Error    : ""
  - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
    Plugin ID       : 125216
    Plugin Name     : Processor Speculative Execution Vulnerabilities [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

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

Plugin Information

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

Plugin Output

tcp/22/ssh

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

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
```

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.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

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

Plugin Output

tcp/22/ssh

```

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

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2022/07/26

Plugin Output

tcp/22/ssh

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

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.).

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: 2022/09/06

Plugin Output

tcp/0

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

  perl-GSSAPI-0.28-9.el7|(none)      Sat Nov  5 01:17:14 2022
  setup-2.8.71-11.el7|(none)      Fri Oct 30 14:22:35 2020
  perl-IO-Socket-IP-0.21-5.el7|(none)      Sat Nov  5 01:17:15 2022
  hwdata-0.252-9.7.el7|(none)      Fri Oct 30 14:23:19 2020
  quota-nls-4.01-19.el7|1      Fri Oct 30 14:22:36 2020
  perl-DBI-1.627-4.el7|(none)      Sat Nov  5 01:17:15 2022
  policycoreutils-python-2.5-34.el7|(none)      Fri Oct 30 14:23:19 2020
  perl-IO-Socket-SSL-1.94-7.el7|(none)      Sat Nov  5 01:17:15 2022
  avahi-libs-0.6.31-20.el7|(none)      Sat Nov  5 01:17:16 2022
  libyaml-0.1.4-11.el7_0|(none)      Fri Oct 30 14:23:20 2020
  libsepol-2.5-10.el7|(none)      Fri Oct 30 14:22:42 2020
  jbigkit-libs-2.0-11.el7|(none)      Sat Nov  5 01:17:16 2022
  info-5.1-5.el7|(none)      Fri Oct 30 14:22:43 2020
  libepoxy-1.5.2-1.el7|(none)      Sat Nov  5 01:17:16 2022
  pakchois-0.4-10.el7|(none)      Sat Nov  5 01:17:17 2022
  libdb-5.3.21-25.el7|(none)      Fri Oct 30 14:22:43 2020
  libdrm-2.4.97-2.el7|(none)      Sat Nov  5 01:17:17 2022
  mod_ssl-2.4.6-97.el7.centos.5|1      Sat Nov  5 01:17:18 2022
  audit-2.8.5-4.el7|(none)      Fri Oct 30 14:23:28 2020
  libcap-2.22-11.el7|(none)      Fri Oct 30 14:22:43 2020
```

```
    graphite2-1.3.10-1.el7_3|(none)      Sat Nov  5 01:17:19 2022
    tcp_wrappers-libs-7.6-77.el7|(none)      Fri Oct 30 14:22:44 2020
    adwaita-cursor-theme-3.28.0-1.el7|(none)      Sat Nov  5 01:17:20 2022
    dracut-config-rescue-033-572.el7|(none)      Fri Oct 30 14:23:30 2020
    keyutils-libs-1.5.8-3.el7|(none)      Fri Oct 30 14:22:44 2020
    gnutls-3.3.29-9.el7_6|(none)      Sat Nov  5 01:17:25 2022
    diffutils-3.3-5.el7|(none)      Fri Oct 30 14:22:44 2020
    subversion-perl-1.7.14-16.el7|(none)      Sat Nov  5 01:17:26 2022
    findutils-4.5.11-6.el7|1      Fri Oct 30 14:22:44 2020
    libXau-1.0.8-2.1.el7|(none)      Sat Nov  5 01:17:26 2022
    libsysfs-2.1.0-16.el7|(none)      Fri Oct 30 14:23:32 2020
    libmnl-1.0.3-7.el7|(none)      Fri  [...]
```

163103 - System Restart Required

Synopsis

The remote system has updates installed which require a reboot.

Description

Using the supplied credentials, Nessus was able to determine that the remote system has updates applied that require a reboot to take effect. Nessus has determined that the system has not been rebooted since these updates have been applied, and thus should be rebooted.

See Also

http://www.nessus.org/u?9e9ce1c1

http://www.nessus.org/u?fd8caec2

Solution

Restart the target system to ensure the updates are applied.

Risk Factor

None

Plugin Information

Published: 2022/07/14, Modified: 2022/07/14

Plugin Output

tcp/0

```
The following security patches require a reboot but have been installed since the most recent system
 boot:

    gnutls-3.3.29-9.el7_6|(none)
```

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.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0502

Plugin Information

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

Plugin Output

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:       'centos'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo


See the output of the following plugin for details :

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

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

User:       'centos'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
reboot   system boot  3.10.0-1160.15.2 Sat Nov  5 01:05 - 14:55 (6+13:49)

wtmp begins Sat Nov  5 01:05:25 2022
```

10287 - 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

udp/0

```
For your information, here is the traceroute from 172.20.0.2 to 3.232.117.195 :
172.20.0.2
172.20.0.1
?

Hop Count: 2
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2022/06/29

Plugin Output

tcp/0

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  1.1  46244  5504 ?        Ss   Nov05   0:09 /usr/lib/systemd/systemd --system
 --deserialize 15
root         2  0.0  0.0      0     0 ?        S    Nov05   0:00 [kthreadd]
root         4  0.0  0.0      0     0 ?        S<   Nov05   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        S    Nov05   0:00 [ksoftirqd/0]
root         7  0.0  0.0      0     0 ?        S    Nov05   0:00 [migration/0]
root         8  0.0  0.0      0     0 ?        S    Nov05   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        R    Nov05   0:02 [rcu_sched]
root        10  0.0  0.0      0     0 ?        S<   Nov05   0:00 [lru-add-drain]
root        11  0.0  0.0      0     0 ?        S    Nov05   0:03 [watchdog/0]
root        13  0.0  0.0      0     0 ?        S    Nov05   0:00 [kdevtmpfs]
root        14  0.0  0.0      0     0 ?        S<   Nov05   0:00 [netns]
root        15  0.0  0.0      0     0 ?        S    Nov05   0:00 [xenwatch]
root        16  0.0  0.0      0     0 ?        S    Nov05   0:00 [xenbus]
root        18  0.0  0.0      0     0 ?        S    Nov05   0:00 [khungtaskd]
root        19  0.0  0.0      0     0 ?        S<   Nov05   0:00 [writeback]
root        20  0.0  0.0      0     0 ?        S<   Nov05   0:00 [kintegrityd]
root        21  0.0  0.0      0     0 ?        S<   Nov05   0:00 [bioset]
root        22  0.0  0.0      0     0 ?        S<   Nov05   0:00 [bioset]
root        23  0.0  0.0      0     0 ?        S<   Nov05   0:00 [bioset]
root        24  0.0  0.0      0     0 ?        S<   Nov05   0:00 [kblockd]
root        25  0.0  0.0      0     0 ?        S<   Nov05   0:00 [md]
root        26  0.0  0.0      0     0 ?        S<   Nov05   0:00 [edac-poller]
root        27  0.0  0.0      0     0 ?        S<   Nov05   0:00 [watchdogd]
root        32  0.0  0.0      0     0 ?        S    Nov05   0:00 [kswapd0]
root        33  0.0  0.0      0     0 ?        SN   Nov05   0:00 [ksmd]
root        34  0.0  0.0      0 [...]
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

  unzip -v                    :
    sh: unzip: command not found


Account  : centos
Protocol : SSH
```