Scan Report

March 29, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scan Mininet". The scan started at Wed Mar 29 12:42:03 2023 UTC and ended at Wed Mar 29 14:35:48 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.41.114	4	5	2	0	0
Total: 1	4	5	2	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 102 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.41.114	SSH	Success	Protocol SSH, Port 22, User cesar

2 Results per Host

2.1 192.168.41.114

Host scan start	Wed Mar 29 12:43:38 2023 UTC
Host scan end	Wed Mar 29 14:35:41 2023 UTC

Service (Port)	Threat Level
package	High
general/tcp	High
package	Medium
general/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 High package

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5958-1)

Summary
The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-5958-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libavcodec58
Installed version:    libavcodec58-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libavcodec58-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libavfilter7
Installed version:    libavfilter7-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libavfilter7-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libavformat58
Installed version:    libavformat58-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libavformat58-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libavutil56
Installed version:    libavutil56-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libavutil56-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libpostproc55
Installed version:    libpostproc55-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libpostproc55-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libswresample3
Installed version:    libswresample3-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libswresample3-7:4.4.2-0ubuntu0.22.04.1+esm1
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.4.2-0ubuntu0.22.04.1
Fixed version:      >=libswscale5-7:4.4.2-0ubuntu0.22.04.1+esm1
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'ffmpeg' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that FFmpeg could be made to dereference a null pointer. An attacker could possibly use this to cause a denial of service via application crash. These issues only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3109, CVE-2022-3341)
It was discovered that FFmpeg could be made to access an out-of-bounds frame by the Apple RPZA encoder. An attacker could possibly use this to cause a denial of service via application crash or access sensitive information. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.10. (CVE-2022-3964)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that FFmpeg could be made to access an out-of-bounds frame by the QuickTime encoder. An attacker could possibly use this to cause a denial of service via application crash or access sensitive information. This issue only affected Ubuntu 22.10. (CVE-2022-3965)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.

Details: `Ubuntu: Security Advisory (USN-5958-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.5958.1

Version used: `2023-03-16T04:11:27Z`

References

```
url: https://ubuntu.com/security/notices/USN-5958-1
url: https://bugs.launchpad.net/ubuntu/+source/ffmpeg/+bug/2007269
cve: CVE-2022-3109
cve: CVE-2022-3341
cve: CVE-2022-3964
cve: CVE-2022-3965
advisory_id: USN-5958-1
cert-bund: WID-SEC-2023-0001
cert-bund: WID-SEC-2022-2363
cert-bund: WID-SEC-2022-2034
dfn-cert: DFN-CERT-2023-0223
dfn-cert: DFN-CERT-2023-0203
dfn-cert: DFN-CERT-2023-0014
dfn-cert: DFN-CERT-2023-0013
dfn-cert: DFN-CERT-2022-2667
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5963-1)

Summary

The remote host is missing an update for the 'vim' package(s) announced via the USN-5963-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.2.3995-1ubuntu2.3
Fixed version:      >=vim-2:8.2.3995-1ubuntu2.4
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.2.3995-1ubuntu2.3
Fixed version:      >=vim-tiny-2:8.2.3995-1ubuntu2.4
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

'vim' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight

It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-47024, CVE-2023-0049, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433)
It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-0051)
It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-1170, CVE-2023-1175)
It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-1264)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5963-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5963.1
Version used: `2023-03-21T04:11:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-5963-1
cve: CVE-2022-47024
cve: CVE-2023-0049
cve: CVE-2023-0051
cve: CVE-2023-0054
cve: CVE-2023-0288
cve: CVE-2023-0433
cve: CVE-2023-1170
cve: CVE-2023-1175
cve: CVE-2023-1264
advisory_id: USN-5963-1
cert-bund: WID-SEC-2023-0596
cert-bund: WID-SEC-2023-0566
cert-bund: WID-SEC-2023-0176
cert-bund: WID-SEC-2023-0168
cert-bund: WID-SEC-2023-0096
cert-bund: WID-SEC-2023-0025
dfn-cert: DFN-CERT-2023-0614
dfn-cert: DFN-CERT-2023-0590
dfn-cert: DFN-CERT-2023-0466
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0308
dfn-cert: DFN-CERT-2023-0237
dfn-cert: DFN-CERT-2023-0231
dfn-cert: DFN-CERT-2023-0230
dfn-cert: DFN-CERT-2023-0043
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5960-1)

Summary
The remote host is missing an update for the 'python2.7, python3.5, python3.6, python3.8, python3.10' package(s) announced via the USN-5960-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python3.10
Installed version:    python3.10-3.10.6-1~22.04.2
Fixed version:      >=python3.10-3.10.6-1~22.04.2ubuntu1
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'python2.7, python3.5, python3.6, python3.8, python3.10' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Yebo Cao discovered that Python incorrectly handled certain URLs. An attacker could possibly use this issue to bypass blocklisting methods by supplying a URL that starts with blank characters.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5960-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5960.1
Version used: `2023-03-17T04:11:07Z`

References

```
url: https://ubuntu.com/security/notices/USN-5960-1
cve: CVE-2023-24329
advisory_id: USN-5960-1
cert-bund: WID-SEC-2023-0513
dfn-cert: DFN-CERT-2023-0571
dfn-cert: DFN-CERT-2023-0552
dfn-cert: DFN-CERT-2023-0527
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0525
```

[return to 192.168.41.114]

2.1.2 High general/tcp

High (CVSS: 7.5)
NVT: Wireshark Security Update (wnpa-sec-2023-08) - Linux

Product detection result

```
cpe:/a:wireshark:wireshark:3.6.2
Detected by Wireshark Version Detection (Linux) (OID: 1.3.6.1.4.1.25623.1.0.8000
↪39)
```

Summary
Wireshark is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 3.6.2
Fixed version:     3.6.12
Installation
path / port:       /usr/bin/wireshark
```

Impact
It may be possible to make Wireshark crash by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.

Solution:
Solution type: VendorFix
Update to version 3.6.12, 4.0.4 or later.

Affected Software/OS
Wireshark version 3.6.0 through 3.6.11, 4.0 through 4.0.3.

Vulnerability Insight
This issue occurs when decoding malformed packets from a pcap file or from the network, causing an out-of-bounds write, resulting in a Denial of Service and limited memory corruption.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Wireshark Security Update (wnpa-sec-2023-08) - Linux`
OID:1.3.6.1.4.1.25623.1.0.124294
Version used: `2023-03-14T10:10:15Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:wireshark:wireshark:3.6.2`
Method: `Wireshark Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800039)

References

```
cve: CVE-2023-1161
url: https://www.wireshark.org/security/wnpa-sec-2023-08.html
url: https://access.redhat.com/security/cve/cve-2023-1161
cert-bund: WID-SEC-2023-0556
dfn-cert: DFN-CERT-2023-0510
```

[return to 192.168.41.114]

2.1.3 Medium package

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-5181-1)

Summary
The remote host is missing an update for the 'jqueryui' package(s) announced via the USN-5181-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjs-jquery-ui
Installed version:    libjs-jquery-ui-1.13.1+dfsg-1
Fixed version:      >=libjs-jquery-ui-1.13.1+dfsg-1ubuntu0.1~esm1
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'jqueryui' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that jQuery UI did not properly validate the values from untrusted sources. An attacker could use this vulnerability to cause a crash or possibly execute arbitrary code. This issue affected only Ubuntu 18.04 ESM and Ubuntu 20.4 ESM. (CVE-2021-41184)
It was discovered that jQuery UI checkboxradio widget did not properly decode certain values from HTML entities. An attacker could possibly use this issue to generate a cross-site scripting(XSS) attack, resulting in a crash or possibly execute arbitrary code. (CVE-2022-31160)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5181-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5181.1
Version used: 2023-01-27T04:10:43Z

References

```
url: https://ubuntu.com/security/notices/USN-5181-1
cve: CVE-2021-41184
cve: CVE-2022-31160
advisory_id: USN-5181-1
cert-bund: WID-SEC-2022-2368
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1778
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1729
cert-bund: WID-SEC-2022-1670
cert-bund: WID-SEC-2022-0760
cert-bund: WID-SEC-2022-0756
cert-bund: WID-SEC-2022-0750
cert-bund: WID-SEC-2022-0749
cert-bund: WID-SEC-2022-0748
cert-bund: WID-SEC-2022-0740
cert-bund: WID-SEC-2022-0737
cert-bund: WID-SEC-2022-0708
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0468
dfn-cert: DFN-CERT-2022-2772
dfn-cert: DFN-CERT-2022-2555
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2281
dfn-cert: DFN-CERT-2022-1616
dfn-cert: DFN-CERT-2022-1613
dfn-cert: DFN-CERT-2022-1612
dfn-cert: DFN-CERT-2022-1206
dfn-cert: DFN-CERT-2022-1142
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0555
dfn-cert: DFN-CERT-2022-0150
dfn-cert: DFN-CERT-2021-2402
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5964-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5964-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.81.0-1ubuntu1.8
Fixed version:      >=curl-7.81.0-1ubuntu1.10
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.81.0-1ubuntu1.8
Fixed version:      >=libcurl3-gnutls-7.81.0-1ubuntu1.10
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.81.0-1ubuntu1.8
Fixed version:      >=libcurl4-7.81.0-1ubuntu1.10
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Harry Sintonen discovered that curl incorrectly handled certain TELNET connection options. Due to lack of proper input scrubbing, curl could pass on user name and telnet options to the server as provided, contrary to expectations. (CVE-2023-27533)
Harry Sintonen discovered that curl incorrectly handled special tilde characters when used with SFTP paths. A remote attacker could possibly use this issue to circumvent filtering. (CVE-2023-27534)
Harry Sintonen discovered that curl incorrectly reused certain FTP connections. This could lead to the wrong credentials being reused, contrary to expectations. (CVE-2023-27535)
Harry Sintonen discovered that curl incorrectly reused connections when the GSS delegation option had been changed. This could lead to the option being reused, contrary to expectations. (CVE-2023-27536)
Harry Sintonen discovered that curl incorrectly reused certain SSH connections. This could lead to the wrong credentials being reused, contrary to expectations. (CVE-2023-27538)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5964-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5964.1
Version used: `2023-03-21T04:11:23Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5964-1
cve: CVE-2023-27533
cve: CVE-2023-27534
cve: CVE-2023-27535
cve: CVE-2023-27536
cve: CVE-2023-27538
advisory_id: USN-5964-1
cert-bund: WID-SEC-2023-0690
dfn-cert: DFN-CERT-2023-0617
```

[return to 192.168.41.114]

2.1.4 Medium general/tcp

Medium (CVSS: 6.5)
NVT: Missing Linux Kernel mitigations for 'RETbleed' hardware vulnerabilities

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Retbleed' hardware vulnerabilities.

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "retbleed"
↪ hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                 | Kernel status (SSH response)
--------------------------------------------------------------------------------
/sys/devices/system/cpu/vulnerabilities/retbleed | Vulnerable
Notes on the "Kernel status / SSH response" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the kernel doesn't know this
↪vulnerability yet and is not providing any mitigation which means the target s
↪ystem is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:

Solution type: VendorFix

Enable the mitigation(s) in the Linux Kernel or update to a more recent Linux Kernel.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'RETbleed' hardware vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.104601
Version used: `2023-03-09T10:09:20Z`

Product Detection Result

Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2022-29900
cve: CVE-2022-29901
url: https://comsec.ethz.ch/research/microarch/retbleed/
url: https://www.intel.com/content/www/us/en/developer/articles/technical/softwa
↪re-security-guidance/advisory-guidance/return-stack-buffer-underflow.html
url: https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1037
cert-bund: WID-SEC-2022-0665
cert-bund: WID-SEC-2022-0659
cert-bund: WID-SEC-2022-0650
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2919
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2609
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2469
dfn-cert: DFN-CERT-2022-2382
dfn-cert: DFN-CERT-2022-1828
dfn-cert: DFN-CERT-2022-1823
dfn-cert: DFN-CERT-2022-1821
dfn-cert: DFN-CERT-2022-1802
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1664
dfn-cert: DFN-CERT-2022-1663
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1598
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1592
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1581
dfn-cert: DFN-CERT-2022-1570
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1568
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1564
dfn-cert: DFN-CERT-2022-1563
dfn-cert: DFN-CERT-2022-1557
dfn-cert: DFN-CERT-2022-1555
dfn-cert: DFN-CERT-2022-1554
```

Medium (CVSS: 5.5)
NVT: Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "spec_stor
↪e_bypass" hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                          | Kernel status (SSH r
↪esponse)
--------------------------------------------------------------------------------
↪--------
/sys/devices/system/cpu/vulnerabilities/spec_store_bypass | Vulnerable
Notes on the "Kernel status / SSH response" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the kernel doesn't know this
↪vulnerability yet and is not providing any mitigation which means the target s
↪ystem is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:

Solution type: VendorFix

Enable the mitigation(s) in the Linux Kernel or update to a more recent Linux Kernel.

Vulnerability Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.

... continues on next page ...

. . . continued from previous page . . .

Details: `Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware .`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.108842
Version used: `2022-07-27T10:11:28Z`

Product Detection Result
Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2018-3639
url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/index.html
cert-bund: CB-K19/0271
cert-bund: CB-K19/0047
cert-bund: CB-K18/1050
cert-bund: CB-K18/0686
cert-bund: CB-K18/0682
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2302
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1767
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1658
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1374
dfn-cert: DFN-CERT-2018-1353
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1323
dfn-cert: DFN-CERT-2018-1304
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1260
dfn-cert: DFN-CERT-2018-1234
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1151
dfn-cert: DFN-CERT-2018-1129
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1105
dfn-cert: DFN-CERT-2018-1042
dfn-cert: DFN-CERT-2018-1041
dfn-cert: DFN-CERT-2018-1025
dfn-cert: DFN-CERT-2018-1023
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0992
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0976
dfn-cert: DFN-CERT-2018-0973
dfn-cert: DFN-CERT-2018-0972
dfn-cert: DFN-CERT-2018-0970
dfn-cert: DFN-CERT-2018-0966
```

Medium (CVSS: 5.5)
NVT: Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

... continues on next page ...

. . . continued from previous page . . .

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities.

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "mmio_stal
↪e_data" hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                    | Kernel status (SSH res
↪ponse)
--------------------------------------------------------------------------------
↪-----------------------------------------------------
/sys/devices/system/cpu/vulnerabilities/mmio_stale_data | Vulnerable: Clear CPU
↪buffers attempted, no microcode; SMT Host state unknown
Notes on the "Kernel status / SSH response" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the kernel doesn't know this
↪vulnerability yet and is not providing any mitigation which means the target s
↪ystem is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:

Solution type: VendorFix

Enable the mitigation(s) in the Linux Kernel or update to a more recent Linux Kernel.

Vulnerability Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.

Details: `Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulne.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.104247

Version used: `2022-07-27T10:11:28Z`

Product Detection Result

Product: `cpe:/a:linux:kernel`

Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`

OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2022-21123
cve: CVE-2022-21125
cve: CVE-2022-21166
url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/processor_mmio_s
↪tale_data.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0336
cert-bund: WID-SEC-2022-0330
cert-bund: WID-SEC-2022-0303
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1664
dfn-cert: DFN-CERT-2022-1663
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1529
dfn-cert: DFN-CERT-2022-1523
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1413
dfn-cert: DFN-CERT-2022-1405
dfn-cert: DFN-CERT-2022-1378
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1365
dfn-cert: DFN-CERT-2022-1358
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1338
dfn-cert: DFN-CERT-2022-1336
dfn-cert: DFN-CERT-2022-1334
dfn-cert: DFN-CERT-2022-1333
dfn-cert: DFN-CERT-2022-1328
```

[return to 192.168.41.114]

2.1.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.41.114]

2.1.6 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3687930852
Packet 2: 3687931914
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP timestamps`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `2020-08-24T08:40:10Z`

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.41.114]

This file was automatically generated.