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 Controller". The scan started at Wed Mar 29 12:42:03 2023 UTC and ended at Wed Mar 29 14:37:04 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
192.168.41.113	20	11	2	0	0
Total: 1	20	11	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 33 results selected by the filtering described above. Before filtering there were 150 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.41.113

Host scan start Wed Mar 29 12:43:38 2023 UTC
Host scan end Wed Mar 29 14:36:58 2023 UTC

Service (Port)	Threat Level
package	High
package	Medium
general/tcp	Medium
8181/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 High package

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5885-1)

Summary
The remote host is missing an update for the 'apr' package(s) announced via the USN-5885-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libapr1
Installed version:    libapr1-1.7.0-8build1
Fixed version:      >=libapr1-1.7.0-8ubuntu0.22.04.1
```

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

Affected Software/OS
'apr' package(s) on Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Ronald Crane discovered integer overflow vulnerabilities in the Apache Portable Runtime (APR) that could potentially result in memory corruption. A remote attacker could possibly use these issues to cause a denial of service or execute arbitary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5885-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5885.1
Version used: `2023-02-27T11:33:27Z`

References
```
url: https://ubuntu.com/security/notices/USN-5885-1
cve: CVE-2022-24963
advisory_id: USN-5885-1
cert-bund: WID-SEC-2023-0245
dfn-cert: DFN-CERT-2023-0531
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5825-2)

Summary
The remote host is missing an update for the 'pam' package(s) announced via the USN-5825-2 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libpam-modules
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    libpam-modules-1.4.0-11ubuntu2.1
Fixed version:      >=libpam-modules-1.4.0-11ubuntu2.3
```

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

Affected Software/OS
'pam' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
USN-5825-1 fixed vulnerabilities in PAM. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that PAM did not correctly restrict login from an IP address that is not resolvable via DNS. An attacker could possibly use this issue to bypass authentication.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5825-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5825.2
Version used: `2023-02-06T15:16:43Z`

References
`url: https://ubuntu.com/security/notices/USN-5825-2`
`url: https://launchpad.net/bugs/2006073`
`cve: CVE-2022-28321`
`advisory_id: USN-5825-2`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5870-1)

Summary
The remote host is missing an update for the 'apr-util' package(s) announced via the USN-5870-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libaprutil1
Installed version:    libaprutil1-1.6.1-5ubuntu4
Fixed version:      >=libaprutil1-1.6.1-5ubuntu4.22.04.1
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'apr-util' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Ronald Crane discovered that APR-util did not properly handled memory when encoding or decoding certain input data. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5870-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5870.1
Version used: `2023-02-15T04:10:50Z`

References
`url: https://ubuntu.com/security/notices/USN-5870-1`
`cve: CVE-2022-25147`
`advisory_id: USN-5870-1`
`cert-bund: WID-SEC-2023-0245`
`dfn-cert: DFN-CERT-2023-0548`
`dfn-cert: DFN-CERT-2023-0302`

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5891-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5891-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.81.0-1ubuntu1.7
Fixed version:      >=curl-7.81.0-1ubuntu1.8
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.81.0-1ubuntu1.7
Fixed version:      >=libcurl3-gnutls-7.81.0-1ubuntu1.8
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.81.0-1ubuntu1.7
Fixed version:      >=libcurl4-7.81.0-1ubuntu1.8
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

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 HSTS support when multiple URLs are requested serially. A remote attacker could possibly use this issue to cause curl to use unencrypted connections. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-23914)
Harry Sintonen discovered that curl incorrectly handled HSTS support when multiple URLs are requested in parallel. A remote attacker could possibly use this issue to cause curl to use unencrypted connections. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-23915)
Patrick Monnerat discovered that curl incorrectly handled memory when processing requests with multi-header compression. A remote attacker could possibly use this issue to cause curl to consume resources, leading to a denial of service. (CVE-2023-23916)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5891-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5891.1
Version used: `2023-03-06T04:11:16Z`

References
`url: https://ubuntu.com/security/notices/USN-5891-1`
`cve: CVE-2023-23914`
`cve: CVE-2023-23915`
`cve: CVE-2023-23916`
`advisory_id: USN-5891-1`
`cert-bund: WID-SEC-2023-0405`
`dfn-cert: DFN-CERT-2023-0385`
`dfn-cert: DFN-CERT-2023-0371`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5851-1)

Summary
The remote host is missing an update for the 'linux, linux-azure, linux-azure-5.15, linux-gkeop, linux-hwe-5.15, linux-ibm, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15, linux-raspi' package(s) announced via the USN-5851-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.15.0.58.56
Fixed version:      >=linux-image-generic-5.15.0.60.58
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'linux, linux-azure, linux-azure-5.15, linux-gkeop, linux-hwe-5.15, linux-ibm, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15, linux-raspi' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that a memory leak existed in the Unix domain socket implementation of the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3543)
It was discovered that the Bluetooth HCI implementation in the Linux kernel did not properly deallocate memory in some situations. An attacker could possibly use this cause a denial of service (memory exhaustion). (CVE-2022-3619)
It was discovered that the hugetlb implementation in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2022-3623)
It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3628)
It was discovered that a use-after-free vulnerability existed in the Bluetooth stack in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3640)
It was discovered that a race condition existed in the SMSC UFX USB driver implementation in the Linux kernel, leading to a use-after-free vulnerability. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41849)
It was discovered that a race condition existed in the Roccat HID driver in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41850)
Tamas Koczka discovered that the Bluetooth L2CAP implementation in the Linux kernel did not properly initialize memory in some situations. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-42895)
Arnaud Gatignol, Quentin Minster, Florent Saudel and Guillaume Teissier discovered that the KSMBD implementation in the Linux kernel did not properly validate user-supplied data in some situations. An authenticated attacker could use this to cause a denial of service (system crash), expose sensitive information (kernel memory) or possibly execute arbitrary code. (CVE-2022-47940)
It was discovered that a race condition existed in the qdisc implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0590)

... 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-5851-1)

OID:1.3.6.1.4.1.25623.1.1.12.2023.5851.1

Version used: 2023-02-10T04:25:54Z

References

url: https://ubuntu.com/security/notices/USN-5851-1
cve: CVE-2022-3543
cve: CVE-2022-3619
cve: CVE-2022-3623
cve: CVE-2022-3628
cve: CVE-2022-3640
cve: CVE-2022-41849
cve: CVE-2022-41850
cve: CVE-2022-42895
cve: CVE-2022-47940
cve: CVE-2023-0590
advisory_id: USN-5851-1
cert-bund: WID-SEC-2023-0322
cert-bund: WID-SEC-2022-2403
cert-bund: WID-SEC-2022-2152
cert-bund: WID-SEC-2022-1903
cert-bund: WID-SEC-2022-1823
cert-bund: WID-SEC-2022-1812
cert-bund: WID-SEC-2022-1761
cert-bund: WID-SEC-2022-1583
dfn-cert: DFN-CERT-2023-0632
dfn-cert: DFN-CERT-2023-0603
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0596
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2023-0500
dfn-cert: DFN-CERT-2023-0485
dfn-cert: DFN-CERT-2023-0447
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0378
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0332
dfn-cert: DFN-CERT-2023-0285
dfn-cert: DFN-CERT-2023-0162
dfn-cert: DFN-CERT-2023-0078
dfn-cert: DFN-CERT-2023-0041
dfn-cert: DFN-CERT-2023-0020
dfn-cert: DFN-CERT-2022-2919
dfn-cert: DFN-CERT-2022-2915

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2913
dfn-cert: DFN-CERT-2022-2905
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2893
dfn-cert: DFN-CERT-2022-2892
dfn-cert: DFN-CERT-2022-2891
dfn-cert: DFN-CERT-2022-2890
dfn-cert: DFN-CERT-2022-2883
dfn-cert: DFN-CERT-2022-2879
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2863
dfn-cert: DFN-CERT-2022-2646
dfn-cert: DFN-CERT-2022-2632
dfn-cert: DFN-CERT-2022-2599
dfn-cert: DFN-CERT-2022-2550
dfn-cert: DFN-CERT-2022-2544
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2274
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5867-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5867-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.38.3-0ubuntu0.22.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.4-0ubuntu0.22.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.38.3-0ubuntu0.22.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.4-0ubuntu0.22.04.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5867-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5867.1
Version used: `2023-03-10T04:12:31Z`

References
`url: https://ubuntu.com/security/notices/USN-5867-1`
`cve: CVE-2022-42826`
`cve: CVE-2023-23517`
`cve: CVE-2023-23518`
`advisory_id: USN-5867-1`
`cert-bund: WID-SEC-2023-0190`
`cert-bund: WID-SEC-2023-0189`
`cert-bund: WID-SEC-2023-0181`
`dfn-cert: DFN-CERT-2023-0448`
`dfn-cert: DFN-CERT-2023-0389`
`dfn-cert: DFN-CERT-2023-0327`
`dfn-cert: DFN-CERT-2023-0264`
`dfn-cert: DFN-CERT-2023-0159`
`dfn-cert: DFN-CERT-2023-0158`
`dfn-cert: DFN-CERT-2023-0157`
`dfn-cert: DFN-CERT-2023-0156`
`dfn-cert: DFN-CERT-2023-0154`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5893-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5893-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.38.3-0ubuntu0.22.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.5-0ubuntu0.22.04.1
```

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.38.3-0ubuntu0.22.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.5-0ubuntu0.22.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5893-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5893.1
Version used: `2023-03-10T04:12:31Z`

References
`url: https://ubuntu.com/security/notices/USN-5893-1`
`cve: CVE-2023-23529`
`advisory_id: USN-5893-1`
`cert-bund: WID-SEC-2023-0358`
`cert-bund: WID-SEC-2023-0355`
`cert-bund: WID-SEC-2023-0347`
`dfn-cert: DFN-CERT-2023-0448`
`dfn-cert: DFN-CERT-2023-0389`
`dfn-cert: DFN-CERT-2023-0380`
`dfn-cert: DFN-CERT-2023-0327`
`dfn-cert: DFN-CERT-2023-0326`
`dfn-cert: DFN-CERT-2023-0325`

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

... continues on next page ...

... continued from previous page ...

```
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)
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

... continues on next page ...

... continued from previous page ...

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).

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

... continues on next page ...

... continued from previous page ...

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`
`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: 7.8)
NVT: Ubuntu: Security Advisory (USN-5912-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.15, linux-azure, linux-azure-5.15, linux-azure-fde, linux-gcp, linux-gcp-5.15, linux-gke, linux-gke-5.15, linux-hwe-5.15, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15' package(s) announced via the USN-5912-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.15.0.58.56
Fixed version:      >=linux-image-generic-5.15.0.67.65
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.15, linux-azure, linux-azure-5.15, linux-azure-fde, linux-gcp, linux-gcp-5.15, linux-gke, linux-gke-5.15, linux-hwe-5.15, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that the Upper Level Protocol (ULP) subsystem in the Linux kernel did not properly handle sockets entering the LISTEN state in certain protocols, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0461)
Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-0179)
It was discovered that the NVMe driver in the Linux kernel did not properly handle reset events in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3169)
Maxim Levitsky discovered that the KVM nested virtualization (SVM) implementation for AMD processors in the Linux kernel did not properly handle nested shutdown execution. An attacker in a guest vm could use this to cause a denial of service (host kernel crash) (CVE-2022-3344)
Gwangun Jung discovered a race condition in the IPv4 implementation in the Linux kernel when deleting multipath routes, resulting in an out-of-bounds read. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3435)
It was discovered that a race condition existed in the Kernel Connection Multiplexor (KCM) socket implementation in the Linux kernel when releasing sockets in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3521)
It was discovered that the Netronome Ethernet driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3545)

... continues on next page ...

... continued from previous page ...

It was discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-4139)
It was discovered that a race condition existed in the Xen network backend driver in the Linux kernel when handling dropped packets in certain circumstances. An attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-42328, CVE-2022-42329)
It was discovered that the NFSD implementation in the Linux kernel contained a use-after-free vulnerability. A remote attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-4379)
It was discovered that a race condition existed in the x86 KVM subsystem implementation in the Linux kernel when nested virtualization and the TDP MMU are enabled. An attacker in a guest vm could use this to cause a denial of service (host OS crash). (CVE-2022-45869)
It ... [Please see the references for more information on the vulnerabilities]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5912-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5912.1
Version used: `2023-03-15T04:11:25Z`

References
`url: https://ubuntu.com/security/notices/USN-5912-1`
`cve: CVE-2022-3169`
`cve: CVE-2022-3344`
`cve: CVE-2022-3435`
`cve: CVE-2022-3521`
`cve: CVE-2022-3545`
`cve: CVE-2022-4139`
`cve: CVE-2022-42328`
`cve: CVE-2022-42329`
`cve: CVE-2022-4379`
`cve: CVE-2022-45869`
`cve: CVE-2022-47518`
`cve: CVE-2022-47519`
`cve: CVE-2022-47520`
`cve: CVE-2022-47521`
`cve: CVE-2023-0179`
`cve: CVE-2023-0461`
`cve: CVE-2023-0468`
`cve: CVE-2023-26605`
`advisory_id: USN-5912-1`
`cert-bund: WID-SEC-2023-0481`
`cert-bund: WID-SEC-2023-0469`
`cert-bund: WID-SEC-2023-0211`
`cert-bund: WID-SEC-2023-0196`
`cert-bund: WID-SEC-2023-0094`
`cert-bund: WID-SEC-2022-2361`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-2324
cert-bund: WID-SEC-2022-2250
cert-bund: WID-SEC-2022-2208
cert-bund: WID-SEC-2022-2197
cert-bund: WID-SEC-2022-1761
cert-bund: WID-SEC-2022-1741
cert-bund: WID-SEC-2022-1648
cert-bund: WID-SEC-2022-1361
dfn-cert: DFN-CERT-2023-0612
dfn-cert: DFN-CERT-2023-0611
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0586
dfn-cert: DFN-CERT-2023-0573
dfn-cert: DFN-CERT-2023-0522
dfn-cert: DFN-CERT-2023-0521
dfn-cert: DFN-CERT-2023-0485
dfn-cert: DFN-CERT-2023-0483
dfn-cert: DFN-CERT-2023-0467
dfn-cert: DFN-CERT-2023-0460
dfn-cert: DFN-CERT-2023-0423
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0367
dfn-cert: DFN-CERT-2023-0342
dfn-cert: DFN-CERT-2023-0333
dfn-cert: DFN-CERT-2023-0331
dfn-cert: DFN-CERT-2023-0324
dfn-cert: DFN-CERT-2023-0273
dfn-cert: DFN-CERT-2023-0272
dfn-cert: DFN-CERT-2023-0194
dfn-cert: DFN-CERT-2023-0193
dfn-cert: DFN-CERT-2023-0185
dfn-cert: DFN-CERT-2023-0183
dfn-cert: DFN-CERT-2023-0182
dfn-cert: DFN-CERT-2023-0168
dfn-cert: DFN-CERT-2023-0167
dfn-cert: DFN-CERT-2023-0162
dfn-cert: DFN-CERT-2023-0143
dfn-cert: DFN-CERT-2023-0094
dfn-cert: DFN-CERT-2023-0086
dfn-cert: DFN-CERT-2022-2919
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2913
dfn-cert: DFN-CERT-2022-2905
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2894

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2893
dfn-cert: DFN-CERT-2022-2892
dfn-cert: DFN-CERT-2022-2891
dfn-cert: DFN-CERT-2022-2890
dfn-cert: DFN-CERT-2022-2887
dfn-cert: DFN-CERT-2022-2886
dfn-cert: DFN-CERT-2022-2885
dfn-cert: DFN-CERT-2022-2884
dfn-cert: DFN-CERT-2022-2883
dfn-cert: DFN-CERT-2022-2882
dfn-cert: DFN-CERT-2022-2880
dfn-cert: DFN-CERT-2022-2879
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2764
dfn-cert: DFN-CERT-2022-2750
dfn-cert: DFN-CERT-2022-2713
dfn-cert: DFN-CERT-2022-2712
dfn-cert: DFN-CERT-2022-2646
dfn-cert: DFN-CERT-2022-2632
dfn-cert: DFN-CERT-2022-2599
dfn-cert: DFN-CERT-2022-2544
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2265
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5900-1)

Summary
The remote host is missing an update for the 'tar' package(s) announced via the USN-5900-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   tar
Installed version:    tar-1.34+dfsg-1build3
Fixed version:      >=tar-1.34+dfsg-1ubuntu0.1.22.04.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'tar' 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 tar incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5900-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5900.1
Version used: `2023-03-02T04:10:54Z`

References
`url: https://ubuntu.com/security/notices/USN-5900-1`
`cve: CVE-2022-48303`
`advisory_id: USN-5900-1`
`cert-bund: WID-SEC-2023-0213`
`dfn-cert: DFN-CERT-2023-0404`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5892-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5892-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.68.2-0ubuntu1.1
Fixed version:      >=libnss3-2:3.68.2-0ubuntu1.2
```

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

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

Vulnerability Insight
It was discovered that NSS incorrectly handled client authentication without a user certificate in the database. A remote attacker could possibly use this issue to cause a NSS client to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-3479)

... continues on next page ...

... continued from previous page ...

Christian Holler discovered that NSS incorrectly handled certain PKCS 12 certificated bundles. A remote attacker could use this issue to cause NSS to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-0767)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5892-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5892.1
Version used: `2023-02-28T04:10:38Z`

References
`url: https://ubuntu.com/security/notices/USN-5892-1`
`cve: CVE-2022-3479`
`cve: CVE-2023-0767`
`advisory_id: USN-5892-1`
`cert-bund: WID-SEC-2023-0407`
`cert-bund: WID-SEC-2023-0385`
`cert-bund: WID-SEC-2022-1708`
`dfn-cert: DFN-CERT-2023-0411`
`dfn-cert: DFN-CERT-2023-0408`
`dfn-cert: DFN-CERT-2023-0395`
`dfn-cert: DFN-CERT-2023-0394`
`dfn-cert: DFN-CERT-2023-0340`
`dfn-cert: DFN-CERT-2023-0139`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5844-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5844-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libssl3
Installed version:    libssl3-3.0.2-0ubuntu1.7
Fixed version:      >=libssl3-3.0.2-0ubuntu1.8
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

David Benjamin discovered that OpenSSL incorrectly handled X.400 address processing. A remote attacker could possibly use this issue to read arbitrary memory contents or cause OpenSSL to crash, resulting in a denial of service. (CVE-2023-0286)
Corey Bonnell discovered that OpenSSL incorrectly handled X.509 certificate verification. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-4203)
Hubert Kario discovered that OpenSSL had a timing based side channel in the OpenSSL RSA Decryption implementation. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2022-4304)
Dawei Wang discovered that OpenSSL incorrectly handled parsing certain PEM data. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2022-4450)
Octavio Galland and Marcel Bohme discovered that OpenSSL incorrectly handled streaming ASN.1 data. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-0215)
Marc Schonefeld discovered that OpenSSL incorrectly handled malformed PKCS7 data. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2023-0216)
Kurt Roeckx discovered that OpenSSL incorrectly handled validating certain DSA public keys. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2023-0217)
Hubert Kario and Dmitry Belyavsky discovered that OpenSSL incorrectly validated certain signatures. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2023-0401)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5844-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5844.1
Version used: `2023-03-13T04:12:15Z`

References
`url: https://ubuntu.com/security/notices/USN-5844-1`
`cve: CVE-2022-4203`
`cve: CVE-2022-4304`
`cve: CVE-2022-4450`
`cve: CVE-2023-0215`
`cve: CVE-2023-0216`
`cve: CVE-2023-0217`
`cve: CVE-2023-0286`
`cve: CVE-2023-0401`
`advisory_id: USN-5844-1`
`cert-bund: WID-SEC-2023-0304`
`dfn-cert: DFN-CERT-2023-0639`
`dfn-cert: DFN-CERT-2023-0618`
`dfn-cert: DFN-CERT-2023-0543`
`dfn-cert: DFN-CERT-2023-0471`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0329
dfn-cert: DFN-CERT-2023-0318
dfn-cert: DFN-CERT-2023-0310
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0288
dfn-cert: DFN-CERT-2023-0284
dfn-cert: DFN-CERT-2023-0283

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5901-1)

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-5901-1 advisory.

Vulnerability Detection Result
Vulnerable package: libgnutls30
Installed version: libgnutls30-3.7.3-4ubuntu1.1
Fixed version: >=libgnutls30-3.7.3-4ubuntu1.2

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

Affected Software/OS
'gnutls28' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Hubert Kario discovered that GnuTLS had a timing side-channel when handling certain RSA messages. A remote attacker could possibly use this issue to recover sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5901-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5901.1
Version used: 2023-03-02T04:10:54Z

References
url: https://ubuntu.com/security/notices/USN-5901-1
cve: CVE-2023-0361
advisory_id: USN-5901-1
cert-bund: WID-SEC-2023-0353
dfn-cert: DFN-CERT-2023-0374

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5945-1)

Summary
The remote host is missing an update for the 'protobuf' package(s) announced via the USN-5945-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libprotobuf23
Installed version:    libprotobuf23-3.12.4-1ubuntu7
Fixed version:      >=libprotobuf23-3.12.4-1ubuntu7.22.04.1
Vulnerable package:   python3-protobuf
Installed version:    python3-protobuf-3.12.4-1ubuntu7
Fixed version:      >=python3-protobuf-3.12.4-1ubuntu7.22.04.1
```

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

Affected Software/OS
'protobuf' package(s) on Ubuntu 14.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that Protocol Buffers did not properly validate field com.google.protobuf.UnknownFieldSet in protobuf-java. An attacker could possibly use this issue to perform a denial of service attack. This issue only affected protobuf Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2021-22569)
It was discovered that Protocol Buffers did not properly parse certain symbols. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. (CVE-2021-22570)
It was discovered that Protocol Buffers did not properly manage memory when parsing specifically crafted messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-1941)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5945-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5945.1
Version used: `2023-03-13T16:21:07Z`

References
```
url: https://ubuntu.com/security/notices/USN-5945-1
cve: CVE-2021-22569
cve: CVE-2021-22570
cve: CVE-2022-1941
advisory_id: USN-5945-1
```

. . . continues on next page . . .

... continued from previous page ...

cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1081
cert-bund: WID-SEC-2022-0607
cert-bund: WID-SEC-2022-0169
cert-bund: CB-K22/0478
cert-bund: CB-K22/0468
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2856
dfn-cert: DFN-CERT-2022-2795
dfn-cert: DFN-CERT-2022-2786
dfn-cert: DFN-CERT-2022-2782
dfn-cert: DFN-CERT-2022-2533
dfn-cert: DFN-CERT-2022-1530
dfn-cert: DFN-CERT-2022-0868
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0345

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5848-1)

Summary
The remote host is missing an update for the 'less' package(s) announced via the USN-5848-1 advisory.

Vulnerability Detection Result
Vulnerable package: less
Installed version: less-590-1build1
Fixed version: >=less-590-1ubuntu0.22.04.1

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

Affected Software/OS
'less' package(s) on Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
David Leadbeater discovered that less was not properly handling escape sequences when displaying raw control characters. A maliciously formed OSC 8 hyperlink could possibly be used by an attacker to cause a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5848-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2023.5848.1
Version used: 2023-02-20T04:10:50Z

References
url: https://ubuntu.com/security/notices/USN-5848-1
cve: CVE-2022-46663
advisory_id: USN-5848-1
dfn-cert: DFN-CERT-2023-0321

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5871-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5871-1 advisory.

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.34.1-1ubuntu1.6
Fixed version: >=git-1:2.34.1-1ubuntu1.8

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

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

Vulnerability Insight
It was discovered that Git incorrectly handled certain repositories. An attacker could use this issue to make Git uses its local clone optimization even when using a non-local transport. (CVE-2023-22490)
Joern Schneeweisz discovered that Git incorrectly handled certain commands. An attacker could possibly use this issue to overwrite a patch outside the working tree. (CVE-2023-23946)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5871-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5871.1
Version used: 2023-02-27T04:10:43Z

References
url: https://ubuntu.com/security/notices/USN-5871-1
cve: CVE-2023-22490
cve: CVE-2023-23946

... continues on next page ...

... continued from previous page ...

advisory_id: USN-5871-1
cert-bund: WID-SEC-2023-0641
cert-bund: WID-SEC-2023-0371
dfn-cert: DFN-CERT-2023-0561
dfn-cert: DFN-CERT-2023-0377
dfn-cert: DFN-CERT-2023-0365

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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0527
dfn-cert: DFN-CERT-2023-0525

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-5921-1)

Summary
The remote host is missing an update for the 'rsync' package(s) announced via the USN-5921-1 advisory.

Vulnerability Detection Result
Vulnerable package: rsync
Installed version: rsync-3.2.3-8ubuntu3.1
Fixed version: >=rsync-3.2.7-0ubuntu0.22.04.2

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

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

Vulnerability Insight
Koen van Hove discovered that the rsync client incorrectly validated filenames returned by servers. If a user or automated system were tricked into connecting to a malicious server, a remote attacker could use this issue to write arbitrary files, and possibly escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5921-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5921.1
Version used: 2023-03-07T04:11:40Z

References
url: https://ubuntu.com/security/notices/USN-5921-1
cve: CVE-2022-29154
advisory_id: USN-5921-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0891
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2115
dfn-cert: DFN-CERT-2022-2078

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1835
dfn-cert: DFN-CERT-2022-1710

High (CVSS: 7.2)
NVT: Ubuntu: Security Advisory (USN-5908-1)

Summary
The remote host is missing an update for the 'sudo' package(s) announced via the USN-5908-1 advisory.

Vulnerability Detection Result
Vulnerable package: sudo
Installed version: sudo-1.9.9-1ubuntu2.2
Fixed version: >=sudo-1.9.9-1ubuntu2.3

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

Affected Software/OS
'sudo' package(s) on Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that Sudo incorrectly handled the per-command chroot feature. In certain environments where Sudo is configured with a rule that contains a CHROOT setting, a local attacker could use this issue to cause Sudo to crash, resulting in a denial of service, or possibly escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5908-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5908.1
Version used: 2023-03-15T04:11:25Z

References
url: https://ubuntu.com/security/notices/USN-5908-1
cve: CVE-2023-27320
advisory_id: USN-5908-1
cert-bund: WID-SEC-2023-0511
dfn-cert: DFN-CERT-2023-0474

[return to 192.168.41.113]

2.1.2 Medium package

Medium (CVSS: 6.8)
NVT: Ubuntu: Security Advisory (USN-5886-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-5886-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   intel-microcode
Installed version:    intel-microcode-3.20220809.0ubuntu0.22.04.1
Fixed version:      >=intel-microcode-3.20230214.0ubuntu0.22.04.1
```

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

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

Vulnerability Insight
Erik C. Bjorge discovered that some Intel(R) Atom and Intel Xeon Scalable Processors did not properly implement access controls for out-of-band management. This may allow a privileged network-adjacent user to potentially escalate privileges. (CVE-2022-21216)
Cfir Cohen, Erdem Aktas, Felix Wilhelm, James Forshaw, Josh Eads, Nagaraju Kodalapura Nagabhushana Rao, Przemyslaw Duda, Liron Shacham and Ron Anderson discovered that some Intel(R) Xeon(R) Processors used incorrect default permissions in some memory controller configurations when using Intel(R) Software Guard Extensions. This may allow a privileged local user to potentially escalate privileges. (CVE-2022-33196)
It was discovered that some 3rd Generation Intel(R) Xeon(R) Scalable Processors did not properly calculate microkey keying. This may allow a privileged local user to potentially disclose information. (CVE-2022-33972)
Joseph Nuzman discovered that some Intel(R) Processors when using Intel(R) Software Guard Extensions did not properly isolate shared resources. This may allow a privileged local user to potentially disclose information. (CVE-2022-38090)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5886-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5886.1
Version used: `2023-03-02T04:10:54Z`

References
```
url: https://ubuntu.com/security/notices/USN-5886-1
cve: CVE-2022-21216
cve: CVE-2022-33196
cve: CVE-2022-33972
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-38090
advisory_id: USN-5886-1
cert-bund: WID-SEC-2023-0393
cert-bund: WID-SEC-2023-0377
dfn-cert: DFN-CERT-2023-0412
dfn-cert: DFN-CERT-2023-0352

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5923-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5923-1 advisory.

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.3.0-6ubuntu0.3
Fixed version: >=libtiff5-4.3.0-6ubuntu0.4

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

Affected Software/OS
'tiff' 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 LibTIFF could be made to read out of bounds when processing certain malformed image files with the tiffcrop tool. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service. (CVE-2023-0795, CVE-2023-0796, CVE-2023-0797, CVE-2023-0798, CVE-2023-0799)
It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files with the tiffcrop tool. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcrop to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-0800, CVE-2023-0801, CVE-2023-0802, CVE-2023-0803, CVE-2023-0804)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5923-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5923.1
Version used: 2023-03-07T04:11:40Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5923-1
cve: CVE-2023-0795
cve: CVE-2023-0796
cve: CVE-2023-0797
cve: CVE-2023-0798
cve: CVE-2023-0799
cve: CVE-2023-0800
cve: CVE-2023-0801
cve: CVE-2023-0802
cve: CVE-2023-0803
cve: CVE-2023-0804
advisory_id: USN-5923-1
cert-bund: WID-SEC-2023-0350
dfn-cert: DFN-CERT-2023-0458
dfn-cert: DFN-CERT-2023-0426
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5928-1)

Summary
The remote host is missing an update for the 'systemd' package(s) announced via the USN-5928-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   systemd
Installed version:    systemd-249.11-0ubuntu3.6
Fixed version:      >=systemd-249.11-0ubuntu3.7
```

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

Affected Software/OS
'systemd' 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 systemd did not properly validate the time and accuracy values provided to the format_timespan() function. An attacker could possibly use this issue to cause a buffer overrun, leading to a denial of service attack. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3821)
It was discovered that systemd did not properly manage the fs.suid_dumpable kernel configurations. A local attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-4415)

... continues on next page ...

... continued from previous page ...

It was discovered that systemd did not properly manage a crash with long backtrace data. A local attacker could possibly use this issue to cause a deadlock, leading to a denial of service attack. This issue only affected Ubuntu 22.10. (CVE-2022-45873)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5928-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5928.1
Version used: `2023-03-07T14:00:00Z`

References
`url: https://ubuntu.com/security/notices/USN-5928-1`
`cve: CVE-2022-3821`
`cve: CVE-2022-4415`
`cve: CVE-2022-45873`
`advisory_id: USN-5928-1`
`cert-bund: WID-SEC-2022-2384`
`cert-bund: WID-SEC-2022-2165`
`cert-bund: WID-SEC-2022-2012`
`dfn-cert: DFN-CERT-2022-2924`
`dfn-cert: DFN-CERT-2022-2897`
`dfn-cert: DFN-CERT-2022-2481`

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5897-1)

Summary
The remote host is missing an update for the 'openjdk-17, openjdk-19, openjdk-lts' package(s) announced via the USN-5897-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jdk
Installed version:    openjdk-11-jdk-11.0.17+8-1ubuntu2~22.04
Fixed version:      >=openjdk-11-jdk-11.0.18+10-0ubuntu1~22.04
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.17+8-1ubuntu2~22.04
Fixed version:      >=openjdk-11-jre-11.0.18+10-0ubuntu1~22.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.17+8-1ubuntu2~22.04
Fixed version:      >=openjdk-11-jre-headless-11.0.18+10-0ubuntu1~22.04
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'openjdk-17, openjdk-19, openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Juraj Somorovsky, Marcel Maehren, Nurullah Erinola, and Robert Merget discovered that the DTLS implementation in the JSSE subsystem of OpenJDK did not properly restrict handshake initiation requests from clients. A remote attacker could possibly use this to cause a denial of service. (CVE-2023-21835)
Markus Loewe discovered that the Java Sound subsystem in OpenJDK did not properly validate the origin of a Soundbank. An attacker could use this to specially craft an untrusted Java application or applet that could load a Soundbank from an attacker controlled remote URL. (CVE-2023-21843)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5897-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5897.1
Version used: `2023-03-02T04:10:54Z`

References
`url: https://ubuntu.com/security/notices/USN-5897-1`
`cve: CVE-2023-21835`
`cve: CVE-2023-21843`
`advisory_id: USN-5897-1`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0128`
`dfn-cert: DFN-CERT-2023-0605`
`dfn-cert: DFN-CERT-2023-0256`
`dfn-cert: DFN-CERT-2023-0217`
`dfn-cert: DFN-CERT-2023-0125`
`dfn-cert: DFN-CERT-2023-0124`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5846-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5846-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:21.1.3-2ubuntu2.6
Fixed version:      >=xserver-xorg-core-2:21.1.3-2ubuntu2.7
Vulnerable package:   xwayland
Installed version:    xwayland-2:22.1.1-1ubuntu0.4
```

... continues on next page ...

... continued from previous page ...

Fixed version: >=xwayland-2:22.1.1-1ubuntu0.5

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

Affected Software/OS
'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain memory operations. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5846-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5846.1
Version used: 2023-02-08T04:10:53Z

References
url: https://ubuntu.com/security/notices/USN-5846-1
cve: CVE-2023-0494
advisory_id: USN-5846-1
cert-bund: WID-SEC-2023-0293
dfn-cert: DFN-CERT-2023-0277

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-7.81.0-1ubuntu1.7
Fixed version: >=curl-7.81.0-1ubuntu1.10
Vulnerable package: libcurl3-gnutls
Installed version: libcurl3-gnutls-7.81.0-1ubuntu1.7
Fixed version: >=libcurl3-gnutls-7.81.0-1ubuntu1.10
Vulnerable package: libcurl4
Installed version: libcurl4-7.81.0-1ubuntu1.7
Fixed version: >=libcurl4-7.81.0-1ubuntu1.10

... continues on next page ...

... continued from previous page ...

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
`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`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5843-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'tmux' package(s) announced via the USN-5843-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:    tmux
Installed version:     tmux-3.2a-4ubuntu0.1
Fixed version:      >=tmux-3.2a-4ubuntu0.2
```

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

Affected Software/OS
'tmux' 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 tmux incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5843-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5843.1
Version used: `2023-02-15T04:10:50Z`

References

```
url: https://ubuntu.com/security/notices/USN-5843-1
cve: CVE-2022-47016
advisory_id: USN-5843-1
dfn-cert: DFN-CERT-2023-0248
```

[return to 192.168.41.113]

2.1.3 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)
```

... 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 '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.

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
```

... continues on next page ...

... continued from previous page ...

```
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
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

... continues on next page ...

... continued from previous page ...

```
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.
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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)
```

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:

... continues on next page ...

... continued from previous page ...

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`
`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`

... continues on next page ...

... continued from previous page ...

```
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 192.168.41.113]

2.1.4 Medium 8181/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
`The following URLs requires Basic Authentication (URL:realm name):`
`http://192.168.41.113:8181/:"karaf"`

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 192.168.41.113]

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.

... continues on next page ...

... continued from previous page ...

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 192.168.41.113]

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
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 407959563
Packet 2: 407960620

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

... continues on next page ...

... continued from previous page ...

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 192.168.41.113]