Scan Report

June 5, 2024

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 "iClean". The scan started at Wed Jun 5 07:14:37 2024 UTC and ended at Wed Jun 5 07:38:31 2024 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
10.10.11.12 capiclean.htb	6	10	3	0	0
Total: 1	6	10	3	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 19 results selected by the filtering described above. Before filtering there were 135 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.10.11.12 - capiclean.htb	SSH	Success	Protocol SSH, Port 22, User root

2 Results per Host

2.1 10.10.11.12

Host scan start	Wed Jun 5 07:15:07 2024 UTC
Host scan end	Wed Jun 5 07:38:25 2024 UTC

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

2.1.1 High package

High (CVSS: 9.8)

NVT: Ubuntu: Security Advisory (USN-6736-1)

Summary
The remote host is missing an update for the 'klibc' package(s) announced via the USN-6736-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   klibc-utils
Installed version:    klibc-utils-2.0.10-4
Fixed version:      >=klibc-utils-2.0.10-4ubuntu0.1
Vulnerable package:   libklibc
Installed version:    libklibc-2.0.10-4
Fixed version:      >=libklibc-2.0.10-4ubuntu0.1
```

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

Affected Software/OS
'klibc' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that zlib, vendored in klibc, incorrectly handled pointer arithmetic. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2016-9840, CVE-2016-9841)
Danilo Ramos discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2018-25032)
Evgeny Legerov discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2022-37434)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6736-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6736.1
Version used: `2024-04-17T04:10:18Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-6736-1
cve: CVE-2016-9840
cve: CVE-2016-9841
cve: CVE-2018-25032
cve: CVE-2022-37434
advisory_id: USN-6736-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0122
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1784
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1031
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0141
cert-bund: WID-SEC-2023-0140
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2023-0125
cert-bund: WID-SEC-2022-1888
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0929
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0736
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0005
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K22/0619
cert-bund: CB-K22/0386
cert-bund: CB-K22/0045
cert-bund: CB-K18/1005
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/1745
cert-bund: CB-K17/1709
cert-bund: CB-K17/1622
cert-bund: CB-K17/1585
cert-bund: CB-K17/1062
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K16/1996
dfn-cert: DFN-CERT-2024-0998
dfn-cert: DFN-CERT-2024-0790
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0430
dfn-cert: DFN-CERT-2023-0122
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2668
dfn-cert: DFN-CERT-2022-2421
dfn-cert: DFN-CERT-2022-2415
dfn-cert: DFN-CERT-2022-2366
dfn-cert: DFN-CERT-2022-2365
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2363
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2066
dfn-cert: DFN-CERT-2022-2059
dfn-cert: DFN-CERT-2022-1992
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1841
dfn-cert: DFN-CERT-2022-1710
dfn-cert: DFN-CERT-2022-1614
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1310
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0768
dfn-cert: DFN-CERT-2022-0716
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2016-2109
```

High (CVSS: 9.8)

NVT: Ubuntu: Security Advisory (USN-6725-1)

Summary

The remote host is missing an update for the 'linux, linux-azure, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.15, linux-ibm, linux-ibm-5.15, linux-intel-iotg, linux-intel-iotg-5.15, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.15, linux-raspi' package(s) announced via the USN-6725-1 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.15.0.101.98
Fixed version:      >=linux-image-generic-5.15.0.102.99
```

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

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

Vulnerability Insight
Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate certain data structure fields when parsing lease contexts, leading to an out-of-bounds read vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1194)
Quentin Minster discovered that a race condition existed in the KSMBD implementation in the Linux kernel, leading to a use-after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32254)
It was discovered that a race condition existed in the KSMBD implementation in the Linux kernel when handling session connections, leading to a use- after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32258)
It was discovered that the KSMBD implementation in the Linux kernel did not properly validate buffer sizes in certain operations, leading to an integer underflow and out-of-bounds read vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-38427)
Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate SMB request protocol IDs, leading to a out-of- bounds read vulnerability. A remote attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-38430)
Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate packet header sizes in certain situations, leading to an out-of-bounds read vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-38431)
It was discovered that the KSMBD implementation in the Linux kernel did not properly handle session setup requests, leading to an out-of-bounds read vulnerability. A remote attacker could use this to expose sensitive information. (CVE-2023-3867)

. . . continues on next page . . .

. . . continued from previous page . . .

Pratyush Yadav discovered that the Xen network backend implementation in the Linux kernel did not properly handle zero length data request, leading to a null pointer dereference vulnerability. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2023-46838)
It was discovered that the IPv6 implementation of the Linux kernel did not properly manage route cache memory usage. A remote attacker could use this to cause a denial of service (memory exhaustion). (CVE-2023-52340)
It was discovered that the device mapper driver in the Linux kernel did not properly validate target size during certain memory allocations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-52429, CVE-2024-23851)
Yang Chaoming ... [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-6725-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6725.1
Version used: `2024-04-10T04:08:49Z`

References

```
url: https://ubuntu.com/security/notices/USN-6725-1
cve: CVE-2023-1194
cve: CVE-2023-32254
cve: CVE-2023-32258
cve: CVE-2023-38427
cve: CVE-2023-38430
cve: CVE-2023-38431
cve: CVE-2023-3867
cve: CVE-2023-46838
cve: CVE-2023-52340
cve: CVE-2023-52429
cve: CVE-2023-52436
cve: CVE-2023-52438
cve: CVE-2023-52439
cve: CVE-2023-52441
cve: CVE-2023-52442
cve: CVE-2023-52443
cve: CVE-2023-52444
cve: CVE-2023-52445
cve: CVE-2023-52448
cve: CVE-2023-52449
cve: CVE-2023-52451
cve: CVE-2023-52454
cve: CVE-2023-52456
cve: CVE-2023-52457
cve: CVE-2023-52458
cve: CVE-2023-52462
cve: CVE-2023-52463
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2023-52464
cve: CVE-2023-52467
cve: CVE-2023-52469
cve: CVE-2023-52470
cve: CVE-2023-52480
cve: CVE-2023-52609
cve: CVE-2023-52610
cve: CVE-2023-52612
cve: CVE-2024-22705
cve: CVE-2024-23850
cve: CVE-2024-23851
cve: CVE-2024-24860
cve: CVE-2024-26586
cve: CVE-2024-26589
cve: CVE-2024-26591
cve: CVE-2024-26597
cve: CVE-2024-26598
cve: CVE-2024-26631
cve: CVE-2024-26633
advisory_id: USN-6725-1
cert-bund: WID-SEC-2024-0654
cert-bund: WID-SEC-2024-0511
cert-bund: WID-SEC-2024-0475
cert-bund: WID-SEC-2024-0473
cert-bund: WID-SEC-2024-0444
cert-bund: WID-SEC-2024-0431
cert-bund: WID-SEC-2024-0345
cert-bund: WID-SEC-2024-0296
cert-bund: WID-SEC-2024-0182
cert-bund: WID-SEC-2024-0177
cert-bund: WID-SEC-2024-0176
cert-bund: WID-SEC-2023-2821
cert-bund: WID-SEC-2023-1865
cert-bund: WID-SEC-2023-1770
cert-bund: WID-SEC-2023-1767
cert-bund: WID-SEC-2023-1255
dfn-cert: DFN-CERT-2024-1231
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1198
dfn-cert: DFN-CERT-2024-1183
dfn-cert: DFN-CERT-2024-1176
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1122
dfn-cert: DFN-CERT-2024-1088
dfn-cert: DFN-CERT-2024-1060
dfn-cert: DFN-CERT-2024-1059
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-1057
dfn-cert: DFN-CERT-2024-1049
dfn-cert: DFN-CERT-2024-1047
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1038
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-1023
dfn-cert: DFN-CERT-2024-1020
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0973
dfn-cert: DFN-CERT-2024-0972
dfn-cert: DFN-CERT-2024-0971
dfn-cert: DFN-CERT-2024-0949
dfn-cert: DFN-CERT-2024-0941
dfn-cert: DFN-CERT-2024-0924
dfn-cert: DFN-CERT-2024-0923
dfn-cert: DFN-CERT-2024-0922
dfn-cert: DFN-CERT-2024-0780
dfn-cert: DFN-CERT-2024-0773
dfn-cert: DFN-CERT-2024-0772
dfn-cert: DFN-CERT-2024-0771
dfn-cert: DFN-CERT-2024-0752
dfn-cert: DFN-CERT-2024-0730
dfn-cert: DFN-CERT-2024-0708
dfn-cert: DFN-CERT-2024-0690
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0683
dfn-cert: DFN-CERT-2024-0658
dfn-cert: DFN-CERT-2024-0490
dfn-cert: DFN-CERT-2024-0434
dfn-cert: DFN-CERT-2024-0432
dfn-cert: DFN-CERT-2024-0431
dfn-cert: DFN-CERT-2024-0430
dfn-cert: DFN-CERT-2024-0429
dfn-cert: DFN-CERT-2024-0414
dfn-cert: DFN-CERT-2024-0413
dfn-cert: DFN-CERT-2024-0410
dfn-cert: DFN-CERT-2024-0409
dfn-cert: DFN-CERT-2024-0407
dfn-cert: DFN-CERT-2024-0403
dfn-cert: DFN-CERT-2024-0259
dfn-cert: DFN-CERT-2024-0173
dfn-cert: DFN-CERT-2023-2995
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2685
dfn-cert: DFN-CERT-2023-2385
dfn-cert: DFN-CERT-2023-2067
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-1872
dfn-cert: DFN-CERT-2023-1870
dfn-cert: DFN-CERT-2023-1541
dfn-cert: DFN-CERT-2023-1405
```

High (CVSS: 7.8)

NVT: Ubuntu: Security Advisory (USN-6766-1)

Summary

The remote host is missing an update for the 'linux, linux-azure, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-ibm, linux-ibm-5.15, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.15' package(s) announced via the USN-6766-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.15.0.101.98
Fixed version:      >=linux-image-generic-5.15.0.106.106
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux, linux-azure, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-ibm, linux-ibm-5.15, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.15' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight

It was discovered that the Open vSwitch implementation in the Linux kernel could overflow its stack during recursive action operations under certain conditions. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-1151)

Sander Wiebing, Alvise de Faveri Tron, Herbert Bos, and Cristiano Giuffrida discovered that the Linux kernel mitigations for the initial Branch History Injection vulnerability (CVE-2022-0001) were insufficient for Intel processors. A local attacker could potentially use this to expose sensitive information. (CVE-2024-2201)

Chenyuan Yang discovered that the RDS Protocol implementation in the Linux kernel contained an out-of-bounds read vulnerability. An attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-23849)

. . . continues on next page . . .

... continued from previous page ...

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems: - PowerPC architecture, - S390 architecture, - Core kernel, - Block layer subsystem, - Android drivers, - Power management core, - Bus devices, - Hardware random number generator core, - Cryptographic API, - Device frequency, - DMA engine subsystem, - ARM SCMI message protocol, - GPU drivers, - HID subsystem, - Hardware monitoring drivers, - I2C subsystem, - IIO ADC drivers, - IIO subsystem, - IIO Magnetometer sensors drivers, - InfiniBand drivers, - Media drivers, - Network drivers, - PCI driver for MicroSemi Switchtec, - PHY drivers, - SCSI drivers, - DesignWare USB3 driver, - BTRFS file system, - Ceph distributed file system, - Ext4 file system, - F2FS file system, - JFS file system, - NILFS2 file system, - NTFS3 file system, - Pstore file system, - SMB network file system, - Memory management, - CAN network layer, - Networking core, - HSR network protocol, - IPv4 networking, - IPv6 networking, - Logical Link layer, - Multipath TCP, - Netfilter, - NFC subsystem, - SMC sockets, - Sun RPC protocol, - TIPC protocol, - Unix domain sockets, - Realtek audio codecs, (CVE-2023-52594, CVE-2023-52601, CVE-2024-26826, CVE-2023-52622, CVE-2024-26665, CVE-2023-52493, CVE-2023-52633, CVE-2024-26684, CVE-2024-26663, CVE-2023-52618, CVE-2023-52588, CVE-2023-52637, CVE-2024-26825, CVE-2023-52606, CVE-2024-26594, CVE-2024-26625, CVE-2024-26720, CVE-2024-26614, CVE-2023-52627, CVE-2023-52602, CVE-2024-26673, CVE-2024-26685, CVE-2023-52638, CVE-2023-52498, CVE-2023-52619, CVE-2024-26910, CVE-2024-26689, CVE-2023-52583, CVE-2024-26676, CVE-2024-26671, CVE-2024-26704, CVE-2024-26608, CVE-2024-26610, CVE-2024-26592, CVE-2023-52599, CVE-2023-52595, CVE-2024-26660, CVE-2023-52617, CVE-2024-26645, CVE-2023-52486, CVE-2023-52631, CVE-2023-52607, CVE-2023-52608, CVE-2024-26722, CVE-2024-26615, CVE-2023-52615, CVE-2024-26636, CVE-2023-52642, CVE-2023-52587, CVE-2024-26712, ... [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-6766-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2024.6766.1

Version used: `2024-05-08T04:07:32Z`

References

```
url: https://ubuntu.com/security/notices/USN-6766-1
cve: CVE-2023-52435
cve: CVE-2023-52486
cve: CVE-2023-52489
cve: CVE-2023-52491
cve: CVE-2023-52492
cve: CVE-2023-52493
cve: CVE-2023-52494
cve: CVE-2023-52498
cve: CVE-2023-52583
cve: CVE-2023-52587
cve: CVE-2023-52588
cve: CVE-2023-52594
cve: CVE-2023-52595
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2023-52597
cve: CVE-2023-52598
cve: CVE-2023-52599
cve: CVE-2023-52601
cve: CVE-2023-52602
cve: CVE-2023-52604
cve: CVE-2023-52606
cve: CVE-2023-52607
cve: CVE-2023-52608
cve: CVE-2023-52614
cve: CVE-2023-52615
cve: CVE-2023-52616
cve: CVE-2023-52617
cve: CVE-2023-52618
cve: CVE-2023-52619
cve: CVE-2023-52622
cve: CVE-2023-52623
cve: CVE-2023-52627
cve: CVE-2023-52631
cve: CVE-2023-52633
cve: CVE-2023-52635
cve: CVE-2023-52637
cve: CVE-2023-52638
cve: CVE-2023-52642
cve: CVE-2023-52643
cve: CVE-2024-1151
cve: CVE-2024-2201
cve: CVE-2024-23849
cve: CVE-2024-26592
cve: CVE-2024-26593
cve: CVE-2024-26594
cve: CVE-2024-26600
cve: CVE-2024-26602
cve: CVE-2024-26606
cve: CVE-2024-26608
cve: CVE-2024-26610
cve: CVE-2024-26614
cve: CVE-2024-26615
cve: CVE-2024-26625
cve: CVE-2024-26627
cve: CVE-2024-26635
cve: CVE-2024-26636
cve: CVE-2024-26640
cve: CVE-2024-26641
cve: CVE-2024-26644
cve: CVE-2024-26645
cve: CVE-2024-26660
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2024-26663
cve: CVE-2024-26664
cve: CVE-2024-26665
cve: CVE-2024-26668
cve: CVE-2024-26671
cve: CVE-2024-26673
cve: CVE-2024-26675
cve: CVE-2024-26676
cve: CVE-2024-26679
cve: CVE-2024-26684
cve: CVE-2024-26685
cve: CVE-2024-26689
cve: CVE-2024-26695
cve: CVE-2024-26696
cve: CVE-2024-26697
cve: CVE-2024-26698
cve: CVE-2024-26702
cve: CVE-2024-26704
cve: CVE-2024-26707
cve: CVE-2024-26712
cve: CVE-2024-26715
cve: CVE-2024-26717
cve: CVE-2024-26720
cve: CVE-2024-26722
cve: CVE-2024-26808
cve: CVE-2024-26825
cve: CVE-2024-26826
cve: CVE-2024-26829
cve: CVE-2024-26910
cve: CVE-2024-26916
cve: CVE-2024-26920
advisory_id: USN-6766-1
cert-bund: WID-SEC-2024-0920
cert-bund: WID-SEC-2024-0913
cert-bund: WID-SEC-2024-0841
cert-bund: WID-SEC-2024-0773
cert-bund: WID-SEC-2024-0749
cert-bund: WID-SEC-2024-0722
cert-bund: WID-SEC-2024-0654
cert-bund: WID-SEC-2024-0632
cert-bund: WID-SEC-2024-0594
cert-bund: WID-SEC-2024-0561
cert-bund: WID-SEC-2024-0527
cert-bund: WID-SEC-2024-0478
cert-bund: WID-SEC-2024-0475
cert-bund: WID-SEC-2024-0474
cert-bund: WID-SEC-2024-0473
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-0444
cert-bund: WID-SEC-2024-0346
cert-bund: WID-SEC-2024-0177
dfn-cert: DFN-CERT-2024-1231
dfn-cert: DFN-CERT-2024-1230
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1183
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1122
dfn-cert: DFN-CERT-2024-1088
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-1023
dfn-cert: DFN-CERT-2024-1020
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0965
dfn-cert: DFN-CERT-2024-0946
dfn-cert: DFN-CERT-2024-0944
dfn-cert: DFN-CERT-2024-0938
dfn-cert: DFN-CERT-2024-0922
dfn-cert: DFN-CERT-2024-0872
dfn-cert: DFN-CERT-2024-0809
dfn-cert: DFN-CERT-2024-0780
dfn-cert: DFN-CERT-2024-0773
dfn-cert: DFN-CERT-2024-0772
dfn-cert: DFN-CERT-2024-0771
dfn-cert: DFN-CERT-2024-0708
dfn-cert: DFN-CERT-2024-0690
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0683
dfn-cert: DFN-CERT-2024-0658
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0655
dfn-cert: DFN-CERT-2024-0490
dfn-cert: DFN-CERT-2024-0434
dfn-cert: DFN-CERT-2024-0295
```

High (CVSS: 7.8)

NVT: Ubuntu: Security Advisory (USN-6742-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.15, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.15, linux-ibm, linux-ibm-5.15, linux-intel-iotg, linux-intel-iotg-5.15, linux-kvm, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15, linux-raspi' package(s) announced via the USN-6742-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.15.0.101.98
Fixed version:      >=linux-image-generic-5.15.0.105.102
```

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

Affected Software/OS

'linux, linux-aws, linux-aws-5.15, linux-azure-5.15, linux-azure-fde, linux-azure-fde-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.15, linux-ibm, linux-ibm-5.15, linux-intel-iotg, linux-intel-iotg-5.15, linux-kvm, linux-lowlatency-hwe-5.15, linux-oracle, linux-oracle-5.15, linux-raspi' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight

Daniele Antonioli discovered that the Secure Simple Pairing and Secure Connections pairing in the Bluetooth protocol could allow an unauthenticated user to complete authentication without pairing credentials. A physically proximate attacker placed between two Bluetooth devices could use this to subsequently impersonate one of the paired devices. (CVE-2023-24023)
Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems: - JFS file system, - Netfilter, (CVE-2024-26581, CVE-2023-52600, CVE-2023-52603)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6742-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6742.1
Version used: `2024-04-22T04:09:21Z`

References

```
url: https://ubuntu.com/security/notices/USN-6742-1
cve: CVE-2023-24023
cve: CVE-2023-52600
cve: CVE-2023-52603
cve: CVE-2024-26581
advisory_id: USN-6742-1
cert-bund: WID-SEC-2024-0561
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-0444
cert-bund: WID-SEC-2023-3043
cert-bund: WID-SEC-2023-2890
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1060
dfn-cert: DFN-CERT-2024-1059
dfn-cert: DFN-CERT-2024-1049
dfn-cert: DFN-CERT-2024-1048
dfn-cert: DFN-CERT-2024-1047
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0658
dfn-cert: DFN-CERT-2023-2820
```

High (CVSS: 7.5)

NVT: Ubuntu: Security Advisory (USN-6735-1)

Summary
The remote host is missing an update for the 'nodejs' package(s) announced via the USN-6735-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnode72
Installed version:    libnode72-12.22.9~dfsg-1ubuntu3.4
Fixed version:      >=libnode72-12.22.9~dfsg-1ubuntu3.5
```

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

Affected Software/OS
'nodejs' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Node.js incorrectly handled the use of invalid public keys while creating an x509 certificate. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.10. (CVE-2023-30588)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that Node.js incorrectly handled the use of CRLF sequences to delimit HTTP requests. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to obtain unauthorised access. This issue only affected Ubuntu 23.10. (CVE-2023-30589)
It was discovered that Node.js incorrectly described the generateKeys() function in the documentation. This inconsistency could possibly lead to security issues in applications that use these APIs. (CVE-2023-30590)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6735-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6735.1
Version used: `2024-04-17T04:10:18Z`

References

```
url: https://ubuntu.com/security/notices/USN-6735-1
cve: CVE-2023-30588
cve: CVE-2023-30589
cve: CVE-2023-30590
advisory_id: USN-6735-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
cert-bund: WID-SEC-2023-1523
dfn-cert: DFN-CERT-2024-0997
dfn-cert: DFN-CERT-2024-0807
dfn-cert: DFN-CERT-2023-3222
dfn-cert: DFN-CERT-2023-2535
dfn-cert: DFN-CERT-2023-2437
dfn-cert: DFN-CERT-2023-2301
dfn-cert: DFN-CERT-2023-1999
dfn-cert: DFN-CERT-2023-1881
dfn-cert: DFN-CERT-2023-1756
dfn-cert: DFN-CERT-2023-1755
dfn-cert: DFN-CERT-2023-1483
dfn-cert: DFN-CERT-2023-1477
dfn-cert: DFN-CERT-2023-1428
```

High (CVSS: 7.5)

NVT: Ubuntu: Security Advisory (USN-6754-1)

Summary
The remote host is missing an update for the 'nghttp2' package(s) announced via the USN-6754-1 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnghttp2-14
Installed version:    libnghttp2-14-1.43.0-1ubuntu0.1
Fixed version:      >=libnghttp2-14-1.43.0-1ubuntu0.2
```

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

Affected Software/OS
'nghttp2' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that nghttp2 incorrectly handled the HTTP/2 implementation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-9511, CVE-2019-9513)
It was discovered that nghttp2 incorrectly handled request cancellation. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2023-44487)
It was discovered that nghttp2 could be made to process an unlimited number of HTTP/2 CONTINUATION frames. A remote attacker could possibly use this issue to cause nghttp2 to consume resources, leading to a denial of service. (CVE-2024-28182)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6754-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6754.1
Version used: `2024-04-26T04:09:00Z`

References

```
url: https://ubuntu.com/security/notices/USN-6754-1
cve: CVE-2019-9511
cve: CVE-2019-9513
cve: CVE-2023-44487
cve: CVE-2024-28182
advisory_id: USN-6754-1
cert-bund: WID-SEC-2024-1050
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0894
cert-bund: WID-SEC-2024-0887
cert-bund: WID-SEC-2024-0874
cert-bund: WID-SEC-2024-0873
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0789
cert-bund: WID-SEC-2024-0597
cert-bund: WID-SEC-2024-0521
cert-bund: WID-SEC-2024-0519
cert-bund: WID-SEC-2024-0123
cert-bund: WID-SEC-2024-0121
cert-bund: WID-SEC-2024-0118
cert-bund: WID-SEC-2024-0117
cert-bund: WID-SEC-2024-0116
cert-bund: WID-SEC-2024-0115
cert-bund: WID-SEC-2024-0108
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2024-0106
cert-bund: WID-SEC-2024-0025
cert-bund: WID-SEC-2023-3146
cert-bund: WID-SEC-2023-2993
cert-bund: WID-SEC-2023-2788
cert-bund: WID-SEC-2023-2723
cert-bund: WID-SEC-2023-2655
cert-bund: WID-SEC-2023-2628
cert-bund: WID-SEC-2023-2627
cert-bund: WID-SEC-2023-2618
cert-bund: WID-SEC-2023-2611
cert-bund: WID-SEC-2023-2606
cert-bund: CB-K19/0733
dfn-cert: DFN-CERT-2024-1252
dfn-cert: DFN-CERT-2024-1238
dfn-cert: DFN-CERT-2024-1105
dfn-cert: DFN-CERT-2024-1016
dfn-cert: DFN-CERT-2024-1002
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0891
dfn-cert: DFN-CERT-2024-0830
dfn-cert: DFN-CERT-2024-0819
dfn-cert: DFN-CERT-2024-0760
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0522
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0464
dfn-cert: DFN-CERT-2024-0398
dfn-cert: DFN-CERT-2024-0367
dfn-cert: DFN-CERT-2024-0337
dfn-cert: DFN-CERT-2024-0149
dfn-cert: DFN-CERT-2024-0134
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0081
dfn-cert: DFN-CERT-2024-0048
dfn-cert: DFN-CERT-2023-3167
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-3119
dfn-cert: DFN-CERT-2023-3073
dfn-cert: DFN-CERT-2023-3059
dfn-cert: DFN-CERT-2023-3035
dfn-cert: DFN-CERT-2023-3007
dfn-cert: DFN-CERT-2023-2996
dfn-cert: DFN-CERT-2023-2991
dfn-cert: DFN-CERT-2023-2971
dfn-cert: DFN-CERT-2023-2959
dfn-cert: DFN-CERT-2023-2912
dfn-cert: DFN-CERT-2023-2892
dfn-cert: DFN-CERT-2023-2882
dfn-cert: DFN-CERT-2023-2876
dfn-cert: DFN-CERT-2023-2864
dfn-cert: DFN-CERT-2023-2851
dfn-cert: DFN-CERT-2023-2849
dfn-cert: DFN-CERT-2023-2787
dfn-cert: DFN-CERT-2023-2785
dfn-cert: DFN-CERT-2023-2730
dfn-cert: DFN-CERT-2023-2729
dfn-cert: DFN-CERT-2023-2708
dfn-cert: DFN-CERT-2023-2696
dfn-cert: DFN-CERT-2023-2695
dfn-cert: DFN-CERT-2023-2680
dfn-cert: DFN-CERT-2023-2677
dfn-cert: DFN-CERT-2023-2675
dfn-cert: DFN-CERT-2023-2670
dfn-cert: DFN-CERT-2023-2666
dfn-cert: DFN-CERT-2023-2646
dfn-cert: DFN-CERT-2023-2637
dfn-cert: DFN-CERT-2023-2636
dfn-cert: DFN-CERT-2023-2635
dfn-cert: DFN-CERT-2023-2623
dfn-cert: DFN-CERT-2023-2603
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2597
dfn-cert: DFN-CERT-2023-2596
dfn-cert: DFN-CERT-2023-2595
dfn-cert: DFN-CERT-2023-2590
dfn-cert: DFN-CERT-2023-2589
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-2586
dfn-cert: DFN-CERT-2023-2585
dfn-cert: DFN-CERT-2023-2572
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-2568
dfn-cert: DFN-CERT-2023-2564
dfn-cert: DFN-CERT-2023-2556
dfn-cert: DFN-CERT-2023-2555
dfn-cert: DFN-CERT-2023-2552
dfn-cert: DFN-CERT-2023-2549
dfn-cert: DFN-CERT-2023-2547
dfn-cert: DFN-CERT-2023-2528
dfn-cert: DFN-CERT-2023-2522
dfn-cert: DFN-CERT-2023-2512
dfn-cert: DFN-CERT-2023-2504
dfn-cert: DFN-CERT-2023-2501
dfn-cert: DFN-CERT-2023-2487
dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2468
dfn-cert: DFN-CERT-2023-2459
dfn-cert: DFN-CERT-2023-2457
dfn-cert: DFN-CERT-2023-2453
dfn-cert: DFN-CERT-2023-2450
dfn-cert: DFN-CERT-2023-2449
dfn-cert: DFN-CERT-2023-2439
dfn-cert: DFN-CERT-2021-0776
dfn-cert: DFN-CERT-2021-0620
dfn-cert: DFN-CERT-2020-2090
dfn-cert: DFN-CERT-2020-1653
dfn-cert: DFN-CERT-2020-1060
dfn-cert: DFN-CERT-2020-0956
dfn-cert: DFN-CERT-2020-0920
dfn-cert: DFN-CERT-2020-0779
dfn-cert: DFN-CERT-2020-0640
dfn-cert: DFN-CERT-2020-0630
dfn-cert: DFN-CERT-2020-0595
dfn-cert: DFN-CERT-2020-0054
dfn-cert: DFN-CERT-2019-2508
dfn-cert: DFN-CERT-2019-2456
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2155
dfn-cert: DFN-CERT-2019-2138
dfn-cert: DFN-CERT-2019-2072
dfn-cert: DFN-CERT-2019-1930
dfn-cert: DFN-CERT-2019-1888
dfn-cert: DFN-CERT-2019-1860
dfn-cert: DFN-CERT-2019-1727
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1690
dfn-cert: DFN-CERT-2019-1689
```

[return to 10.10.11.12]

2.1.2 Medium package

Medium (CVSS: 6.5)

NVT: Ubuntu: Security Advisory (USN-6727-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-6727-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.68.2-0ubuntu1.2
Fixed version:      >=libnss3-2:3.98-0ubuntu0.22.04.1
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that NSS incorrectly handled padding when checking PKCS#1 certificates. A remote attacker could possibly use this issue to perform Bleichenbacher-like attacks and recover private data. This issue only affected Ubuntu 20.04 LTS. (CVE-2023-4421)
It was discovered that NSS had a timing side-channel when performing RSA decryption. A remote attacker could possibly use this issue to recover private data. (CVE-2023-5388)
It was discovered that NSS had a timing side-channel when using certain NIST curves. A remote attacker could possibly use this issue to recover private data. (CVE-2023-6135)
The NSS package contained outdated CA certificates. This update refreshes the NSS package to version 3.98 which includes the latest CA certificate bundle and other security improvements.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6727-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6727.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2024-04-11T04:08:46Z

References

```
url: https://ubuntu.com/security/notices/USN-6727-1
cve: CVE-2023-4421
cve: CVE-2023-5388
cve: CVE-2023-6135
advisory_id: USN-6727-1
cert-bund: WID-SEC-2024-0669
cert-bund: WID-SEC-2024-0045
cert-bund: WID-SEC-2023-3185
cert-bund: WID-SEC-2023-2787
dfn-cert: DFN-CERT-2024-1071
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0955
dfn-cert: DFN-CERT-2024-0898
dfn-cert: DFN-CERT-2024-0836
dfn-cert: DFN-CERT-2024-0815
dfn-cert: DFN-CERT-2024-0796
dfn-cert: DFN-CERT-2024-0795
dfn-cert: DFN-CERT-2024-0784
dfn-cert: DFN-CERT-2024-0735
dfn-cert: DFN-CERT-2024-0734
dfn-cert: DFN-CERT-2024-0647
dfn-cert: DFN-CERT-2024-0369
dfn-cert: DFN-CERT-2024-0069
dfn-cert: DFN-CERT-2023-3180
dfn-cert: DFN-CERT-2023-3106
dfn-cert: DFN-CERT-2023-2661
```

Medium (CVSS: 6.5)

NVT: Ubuntu: Security Advisory (USN-6727-2)

Summary

The remote host is missing an update for the 'nss' package(s) announced via the USN-6727-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.68.2-0ubuntu1.2
Fixed version:      >=libnss3-2:3.98-0ubuntu0.22.04.2
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

Vulnerability Insight
USN-6727-1 fixed vulnerabilities in NSS. The update introduced a regression when trying to load security modules on Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. This update fixes the problem. We apologize for the inconvenience.
Original advisory details:
It was discovered that NSS incorrectly handled padding when checking PKCS#1 certificates. A remote attacker could possibly use this issue to perform Bleichenbacher-like attacks and recover private data. This issue only affected Ubuntu 20.04 LTS. (CVE-2023-4421)
It was discovered that NSS had a timing side-channel when performing RSA decryption. A remote attacker could possibly use this issue to recover private data. (CVE-2023-5388)
It was discovered that NSS had a timing side-channel when using certain NIST curves. A remote attacker could possibly use this issue to recover private data. (CVE-2023-6135)
The NSS package contained outdated CA certificates. This update refreshes the NSS package to version 3.98 which includes the latest CA certificate bundle and other security improvements.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6727-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6727.2
Version used: `2024-04-12T04:08:49Z`

References

```
url: https://ubuntu.com/security/notices/USN-6727-2
url: https://launchpad.net/bugs/2060906
cve: CVE-2023-4421
cve: CVE-2023-5388
cve: CVE-2023-6135
advisory_id: USN-6727-2
cert-bund: WID-SEC-2024-0669
cert-bund: WID-SEC-2024-0045
cert-bund: WID-SEC-2023-3185
cert-bund: WID-SEC-2023-2787
dfn-cert: DFN-CERT-2024-1071
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0955
dfn-cert: DFN-CERT-2024-0898
dfn-cert: DFN-CERT-2024-0836
dfn-cert: DFN-CERT-2024-0815
dfn-cert: DFN-CERT-2024-0796
dfn-cert: DFN-CERT-2024-0795
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-0784
dfn-cert: DFN-CERT-2024-0735
dfn-cert: DFN-CERT-2024-0734
dfn-cert: DFN-CERT-2024-0647
dfn-cert: DFN-CERT-2024-0369
dfn-cert: DFN-CERT-2024-0069
dfn-cert: DFN-CERT-2023-3180
dfn-cert: DFN-CERT-2023-3106
dfn-cert: DFN-CERT-2023-2661
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6719-2)

Summary
The remote host is missing an update for the 'util-linux' package(s) announced via the USN-6719-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   util-linux
Installed version:    util-linux-2.37.2-4ubuntu3.3
Fixed version:      >=util-linux-2.37.2-4ubuntu3.4
```

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

Affected Software/OS
'util-linux' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
USN-6719-1 fixed a vulnerability in util-linux. Unfortunately, it was discovered that the fix did not fully address the issue. This update removes the setgid permission bit from the wall and write utilities.
Original advisory details:
Skyler Ferrante discovered that the util-linux wall command did not filter escape sequences from command line arguments. A local attacker could possibly use this issue to obtain sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6719-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6719.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2024-04-11T04:08:46Z

References

```
url: https://ubuntu.com/security/notices/USN-6719-2
cve: CVE-2024-28085
advisory_id: USN-6719-2
cert-bund: WID-SEC-2024-0734
dfn-cert: DFN-CERT-2024-0903
dfn-cert: DFN-CERT-2024-0826
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6729-1)

Summary

The remote host is missing an update for the 'apache2' package(s) announced via the USN-6729-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.52-1ubuntu4.8
Fixed version:      >=apache2-2.4.52-1ubuntu4.9
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'apache2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight

Orange Tsai discovered that the Apache HTTP Server incorrectly handled validating certain input. A remote attacker could possibly use this issue to perform HTTP request splitting attacks. (CVE-2023-38709)

Keran Mu and Jianjun Chen discovered that the Apache HTTP Server incorrectly handled validating certain input. A remote attacker could possibly use this issue to perform HTTP request splitting attacks. (CVE-2024-24795)

Bartek Nowotarski discovered that the Apache HTTP Server HTTP/2 module incorrectly handled endless continuation frames. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. (CVE-2024-27316)

Vulnerability Detection Method

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Ubuntu: Security Advisory (USN-6729-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6729.1
Version used: `2024-04-12T04:08:49Z`

References

```
url: https://ubuntu.com/security/notices/USN-6729-1
cve: CVE-2023-38709
cve: CVE-2024-24795
cve: CVE-2024-27316
advisory_id: USN-6729-1
cert-bund: WID-SEC-2024-0801
cert-bund: WID-SEC-2024-0789
dfn-cert: DFN-CERT-2024-1238
dfn-cert: DFN-CERT-2024-1031
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2024-0964
dfn-cert: DFN-CERT-2024-0901
dfn-cert: DFN-CERT-2024-0890
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6755-1)

Summary
The remote host is missing an update for the 'cpio' package(s) announced via the USN-6755-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   cpio
Installed version:    cpio-2.13+dfsg-7
Fixed version:      >=cpio-2.13+dfsg-7ubuntu0.1
```

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

Affected Software/OS
'cpio' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Ingo Bruckl discovered that cpio contained a path traversal vulnerability. If a user or automated system were tricked into extracting a specially crafted cpio archive, an attacker could possibly use this issue to write arbitrary files outside the target directory on the host, even if using the option –no-absolute-filenames.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6755-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6755.1
Version used: `2024-04-30T04:09:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-6755-1
cve: CVE-2023-7207
advisory_id: USN-6755-1
cert-bund: WID-SEC-2024-0245
dfn-cert: DFN-CERT-2024-0252
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6756-1)

Summary

The remote host is missing an update for the 'less' package(s) announced via the USN-6756-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   less
Installed version:    less-590-1ubuntu0.22.04.2
Fixed version:      >=less-590-1ubuntu0.22.04.3
```

Solution:

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

Affected Software/OS

'less' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that less mishandled newline characters in file names. If a user or automated system were tricked into opening specially crafted files, an attacker could possibly use this issue to execute arbitrary commands on the host.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6756-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6756.1
Version used: `2024-04-30T04:09:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-6756-1
cve: CVE-2024-32487
advisory_id: USN-6756-1
cert-bund: WID-SEC-2024-0880
dfn-cert: DFN-CERT-2024-1210
dfn-cert: DFN-CERT-2024-1129
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6737-1)

Summary

The remote host is missing an update for the 'glibc' package(s) announced via the USN-6737-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libc6
Installed version:    libc6-2.35-0ubuntu3.6
Fixed version:      >=libc6-2.35-0ubuntu3.7
```

Solution:

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

Affected Software/OS

'glibc' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight

Charles Fol discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code.

. . . 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-6737-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6737.1
Version used: `2024-04-19T04:08:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-6737-1
cve: CVE-2024-2961
advisory_id: USN-6737-1
cert-bund: WID-SEC-2024-0926
dfn-cert: DFN-CERT-2024-1254
dfn-cert: DFN-CERT-2024-1195
dfn-cert: DFN-CERT-2024-1040
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6768-1)

Summary

The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-6768-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.72.4-0ubuntu2.2
Fixed version:      >=libglib2.0-0-2.72.4-0ubuntu2.3
Vulnerable package:   libglib2.0-bin
Installed version:    libglib2.0-bin-2.72.4-0ubuntu2.2
Fixed version:      >=libglib2.0-bin-2.72.4-0ubuntu2.3
```

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

Affected Software/OS

'glib2.0' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight

Alicia Boya Garcia discovered that GLib incorrectly handled signal subscriptions. A local attacker could use this issue to spoof D-Bus signals resulting in a variety of impacts including possible privilege escalation.

. . . 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-6768-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6768.1
Version used: `2024-05-10T04:07:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-6768-1
cve: CVE-2024-34397
advisory_id: USN-6768-1
dfn-cert: DFN-CERT-2024-1227
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6733-1)

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-6733-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgnutls30
Installed version:    libgnutls30-3.7.3-4ubuntu1.4
Fixed version:      >=libgnutls30-3.7.3-4ubuntu1.5
```

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

Affected Software/OS
'gnutls28' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that GnuTLS had a timing side-channel when performing certain ECDSA operations. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2024-28834)
It was discovered that GnuTLS incorrectly handled verifying certain PEM bundles. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2024-28835)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6733-1)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2024.6733.1
Version used: `2024-04-16T04:09:00Z`

References

```
url: https://ubuntu.com/security/notices/USN-6733-1
cve: CVE-2024-28834
cve: CVE-2024-28835
advisory_id: USN-6733-1
cert-bund: WID-SEC-2024-0686
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-1072
dfn-cert: DFN-CERT-2024-0975
dfn-cert: DFN-CERT-2024-0754
```

[return to 10.10.11.12]

2.1.3 Medium 80/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.

Quality of Detection: 80

Vulnerability Detection Result

```
The following input fields were identified (URL:input name):
http://capiclean.htb/login:password
```

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: `2023-09-07T05:05:21Z`

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 10.10.11.12]

2.1.4 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely

. . . continues on next page . . .

. . . continued from previous page . . .

- 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.

Vulnerability Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 10.10.11.12]

2.1.5 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary

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

Quality of Detection: 80

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: 1300911490
Packet 2: 1300912649
```

Impact

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

. . . continues on next page . . .

. . . continued from previous page . . .

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 10.10.11.12]

2.1.6 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection: 80

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2023-10-12T05:05:32Z`

References

url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 10.10.11.12]