Scan Report

June 17, 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 "forensics". The scan started at Mon Jun 17 00:55:33 2024 UTC and ended at Mon Jun 17 03:48:30 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
192.168.218.129 SIFTWORKSTATION	438	171	10	0	0
Total: 1	438	171	10	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 619 results selected by the filtering described above. Before filtering there were 878 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.218.129 - SIFTWORKSTATION	SSH	Success	Protocol SSH, Port 22, User sansforensics, 'su' Us
192.168.218.129 - SIFTWORKSTATION	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.218.129

Host scan start	Mon Jun 17 00:56:01 2024 UTC
Host scan end	Mon Jun 17 03:48:24 2024 UTC

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

2.1.1 High package

High (CVSS: 10.0)
NVT: Ubuntu: Security Advisory (USN-6125-1)

Summary
The remote host is missing an update for the 'snapd' package(s) announced via the USN-6125-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   snapd
Installed version:    snapd-2.49.2+20.04
Fixed version:      >=snapd-2.58+20.04.1
```

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

Affected Software/OS
'snapd' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that the snap sandbox did not restrict the use of the ioctl system call with a TIOCLINUX request. This could be exploited by a malicious snap to inject commands into the controlling terminal which would then be executed outside of the snap sandbox once the snap had exited. This could allow an attacker to execute arbitrary commands outside of the confined snap sandbox. Note: graphical terminal emulators like xterm, gnome-terminal and others are not affected - this can only be exploited when snaps are run on a virtual console.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6125-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6125.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6125-1
cve: CVE-2023-1523
advisory_id: USN-6125-1
cert-bund: WID-SEC-2023-1329
dfn-cert: DFN-CERT-2023-1234
```

High (CVSS: 10.0)
NVT: Ubuntu: Security Advisory (USN-5229-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5229-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-96.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information across domains, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5229-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5229.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5229-1
cve: CVE-2021-4140
cve: CVE-2022-22737
cve: CVE-2022-22738
cve: CVE-2022-22739
cve: CVE-2022-22740
cve: CVE-2022-22741
cve: CVE-2022-22742
cve: CVE-2022-22743
cve: CVE-2022-22745
cve: CVE-2022-22747
cve: CVE-2022-22748
cve: CVE-2022-22751
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-22752
advisory_id: USN-5229-1
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2022-0611
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0039
dfn-cert: DFN-CERT-2022-1524
dfn-cert: DFN-CERT-2022-0452
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0187
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2022-0046
dfn-cert: DFN-CERT-2022-0045

High (CVSS: 10.0)
NVT: Ubuntu: Security Advisory (USN-5248-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5248-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:91.5.0+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, conduct header splitting attacks, conduct spoofing attacks, bypass security restrictions, confuse the user, or execute arbitrary code. (CVE-2021-4129, CVE-2021-4140, CVE-2021-29981, CVE-2021-29982, CVE-2021-29987, CVE-2021-29991, CVE-2021-38495, CVE-2021-38496, CVE-2021-38497, CVE-2021-38498, CVE-2021-38500, CVE-2021-38501, CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509, CVE-2021-43534, CVE-2021-43535, CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43656, CVE-2022-22737, CVE-2022-22738, CVE-2022-22739, CVE-2022-22740, CVE-2022-22741, CVE-2022-22742, CVE-2022-22743, CVE-2022-22745, CVE-2022-22747, CVE-2022-22748, CVE-2022-22751)
It was discovered that Thunderbird ignored the configuration to require STARTTLS for an SMTP connection. A person-in-the-middle could potentially exploit this to perform a downgrade attack in order to intercept messages or take control of a session. (CVE-2021-38502)
It was discovered that JavaScript was unexpectedly enabled in the composition area. An attacker could potentially exploit this in combination with another vulnerability, with unspecified impacts. (CVE-2021-43528)
A buffer overflow was discovered in the Matrix chat library bundled with Thunderbird. An attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. (CVE-2021-44538)
It was discovered that Thunderbird's OpenPGP integration only considered the inner signed message when checking signature validity in a message that contains an additional outer MIME layer. An attacker could potentially exploit this to trick the user into thinking that a message has a valid signature. (CVE-2021-4126)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5248-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5248.1
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-5248-1`
`cve: CVE-2021-29981`
`cve: CVE-2021-29982`
`cve: CVE-2021-29987`
`cve: CVE-2021-29991`
`cve: CVE-2021-38495`
`cve: CVE-2021-38496`
`cve: CVE-2021-38497`
`cve: CVE-2021-38498`
`cve: CVE-2021-38500`
`cve: CVE-2021-38501`
`cve: CVE-2021-38502`
`cve: CVE-2021-38503`

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-38504
cve: CVE-2021-38506
cve: CVE-2021-38507
cve: CVE-2021-38508
cve: CVE-2021-38509
cve: CVE-2021-4126
cve: CVE-2021-4129
cve: CVE-2021-4140
cve: CVE-2021-43528
cve: CVE-2021-43534
cve: CVE-2021-43535
cve: CVE-2021-43536
cve: CVE-2021-43537
cve: CVE-2021-43538
cve: CVE-2021-43539
cve: CVE-2021-43541
cve: CVE-2021-43542
cve: CVE-2021-43543
cve: CVE-2021-43545
cve: CVE-2021-43546
cve: CVE-2021-44538
cve: CVE-2022-22737
cve: CVE-2022-22738
cve: CVE-2022-22739
cve: CVE-2022-22740
cve: CVE-2022-22741
cve: CVE-2022-22742
cve: CVE-2022-22743
cve: CVE-2022-22745
cve: CVE-2022-22747
cve: CVE-2022-22748
cve: CVE-2022-22751
advisory_id: USN-5248-1
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2022-1029
cert-bund: WID-SEC-2022-1028
cert-bund: WID-SEC-2022-1024
cert-bund: WID-SEC-2022-1022
cert-bund: WID-SEC-2022-0689
cert-bund: WID-SEC-2022-0611
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0039
cert-bund: CB-K21/1300
cert-bund: CB-K21/1255
cert-bund: CB-K21/1141
cert-bund: CB-K21/1045

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K21/0939
cert-bund: CB-K21/0884
cert-bund: CB-K21/0861
dfn-cert: DFN-CERT-2022-1524
dfn-cert: DFN-CERT-2022-0452
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0187
dfn-cert: DFN-CERT-2022-0110
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2022-0046
dfn-cert: DFN-CERT-2022-0045
dfn-cert: DFN-CERT-2021-2655
dfn-cert: DFN-CERT-2021-2642
dfn-cert: DFN-CERT-2021-2599
dfn-cert: DFN-CERT-2021-2586
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2549
dfn-cert: DFN-CERT-2021-2548
dfn-cert: DFN-CERT-2021-2294
dfn-cert: DFN-CERT-2021-2277
dfn-cert: DFN-CERT-2021-2124
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2075
dfn-cert: DFN-CERT-2021-1889
dfn-cert: DFN-CERT-2021-1888
dfn-cert: DFN-CERT-2021-1762
dfn-cert: DFN-CERT-2021-1732
dfn-cert: DFN-CERT-2021-1695

High (CVSS: 10.0)
NVT: Ubuntu: Security Advisory (USN-5131-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5131-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-94.0+build3-0ubuntu0.20.04.1

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, spoof the browser UI, confuse the user, conduct phishing attacks, or execute arbitrary code. (CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509)
It was discovered that the 'Copy Image Link' context menu action would copy the final image URL after redirects. If a user were tricked into copying and pasting a link for an embedded image that triggered authentication flows back to the page, an attacker could potentially exploit this to steal authentication tokens.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5131-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5131.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5131-1`
`cve: CVE-2021-38503`
`cve: CVE-2021-38504`
`cve: CVE-2021-38506`
`cve: CVE-2021-38507`
`cve: CVE-2021-38508`
`cve: CVE-2021-38509`
`advisory_id: USN-5131-1`
`cert-bund: WID-SEC-2023-0839`
`cert-bund: WID-SEC-2022-1028`
`cert-bund: CB-K21/1141`
`dfn-cert: DFN-CERT-2022-0068`
`dfn-cert: DFN-CERT-2021-2586`
`dfn-cert: DFN-CERT-2021-2294`
`dfn-cert: DFN-CERT-2021-2277`

High (CVSS: 9.9)
NVT: Ubuntu: Security Advisory (USN-5075-1)

Summary
The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-5075-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   ghostscript
Installed version:    ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version:      >=ghostscript-9.50~dfsg-5ubuntu4.3
Vulnerable package:   libgs9
Installed version:    libgs9-9.50~dfsg-5ubuntu4.2
Fixed version:      >=libgs9-9.50~dfsg-5ubuntu4.3
```

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

Affected Software/OS
'ghostscript' package(s) on Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to access arbitrary files, execute arbitrary code, or 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-5075-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5075.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5075-1
cve: CVE-2021-3781
advisory_id: USN-5075-1
cert-bund: WID-SEC-2022-2137
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-1910
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5726-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5726-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-107.0+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the contents of the addressbar, bypass security restrictions, cross-site tracing or execute arbitrary code. (CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45407, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45413, CVE-2022-40674, CVE-2022-45418, CVE-2022-45419, CVE-2022-45420, CVE-2022-45421)
Armin Ebert discovered that Firefox did not properly manage while resolving file symlink. If a user were tricked into opening a specially crafted weblink, an attacker could potentially exploit these to cause a denial of service. (CVE-2022-45412)
Jefferson Scher and Jayateertha Guruprasad discovered that Firefox did not properly sanitize the HTML download file extension under certain circumstances. If a user were tricked into downloading and executing malicious content, a remote attacker could execute arbitrary code with the privileges of the user invoking the programs. (CVE-2022-45415)
Erik Kraft, Martin Schwarzl, and Andrew McCreight discovered that Firefox incorrectly handled keyboard events. An attacker could possibly use this issue to perform a timing side-channel attack and possibly figure out which keys are being pressed. (CVE-2022-45416)
Kagami discovered that Firefox did not detect Private Browsing Mode correctly. An attacker could possibly use this issue to obtain sensitive information about Private Browsing Mode. (CVE-2022-45417)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5726-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5726.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5726-1
cve: CVE-2022-40674
cve: CVE-2022-45403
cve: CVE-2022-45404

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-45405
cve: CVE-2022-45406
cve: CVE-2022-45407
cve: CVE-2022-45408
cve: CVE-2022-45409
cve: CVE-2022-45410
cve: CVE-2022-45411
cve: CVE-2022-45412
cve: CVE-2022-45413
cve: CVE-2022-45415
cve: CVE-2022-45416
cve: CVE-2022-45417
cve: CVE-2022-45418
cve: CVE-2022-45419
cve: CVE-2022-45420
cve: CVE-2022-45421
advisory_id: USN-5726-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2055
cert-bund: WID-SEC-2022-1504
dfn-cert: DFN-CERT-2023-1919
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0666
dfn-cert: DFN-CERT-2023-0150
dfn-cert: DFN-CERT-2022-2821
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2664
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2576
dfn-cert: DFN-CERT-2022-2575
dfn-cert: DFN-CERT-2022-2344
dfn-cert: DFN-CERT-2022-2343
dfn-cert: DFN-CERT-2022-2264
dfn-cert: DFN-CERT-2022-2218
dfn-cert: DFN-CERT-2022-2207
dfn-cert: DFN-CERT-2022-2120
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5942-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5942-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: apache2
Installed version: apache2-2.4.41-4ubuntu3.3
Fixed version: >=apache2-2.4.41-4ubuntu3.14

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Lars Krapf discovered that the Apache HTTP Server mod_proxy module incorrectly handled certain configurations. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2023-25690)
Dimas Fariski Setyawan Putra discovered that the Apache HTTP Server mod_proxy_uwsgi module incorrectly handled certain special characters. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2023-27522)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5942-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5942.1
Version used: 2024-02-02T04:09:01Z

References
cve: CVE-2023-27522
url: https://ubuntu.com/security/notices/USN-5942-1
cve: CVE-2023-25690
advisory_id: USN-5942-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-3129
cert-bund: WID-SEC-2023-2694
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1809
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0657
cert-bund: WID-SEC-2023-0583
dfn-cert: DFN-CERT-2023-1895

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1232
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0788
dfn-cert: DFN-CERT-2023-0658
dfn-cert: DFN-CERT-2023-0546

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5168-2)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5168-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:78.14.0+build1-0ubuntu0.20.04.2

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Tavis Ormandy discovered that NSS, included with Thunderbird, incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause Thunderbird to crash, resulting in 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-5168-2)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5168.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5168-2
cve: CVE-2021-43527
advisory_id: USN-5168-2
cert-bund: WID-SEC-2024-0114

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1766
cert-bund: WID-SEC-2022-0810
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1246
dfn-cert: DFN-CERT-2024-0126
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-1105
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2021-2642
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2563
dfn-cert: DFN-CERT-2021-2499

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5205-1)

Summary
The remote host is missing an update for the 'tcpreplay' package(s) announced via the USN-5205-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: tcpreplay
Installed version: tcpreplay-4.3.2-1build1
Fixed version: >=tcpreplay-4.3.2-1ubuntu0.1~esm2

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

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

Vulnerability Insight
It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input when processed by tcpprep. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 ESM. (CVE-2018-13112)

... continues on next page ...

... continued from previous page ...

It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. This issue only affected Ubuntu 16.04 ESM and Ubuntu 18.04 ESM. (CVE-2018-17580, CVE-2018-17582)
It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 ESM and Ubuntu 18.04 ESM. (CVE-2018-17974, CVE-2018-18407)
It was discovered that a use-after-free existed in Tcpreplay in the tcpbridge binary. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 ESM and Ubuntu 18.04 ESM. (CVE-2018-18408)
It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2018-20552, CVE-2018-20553)
It was discovered that a heap-based buffer over-read that existed in Tcpreplay caused an application crash when tcprewrite or tcpreplay-edit received specially crafted packet capture input. An attacker could possibly use this to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2020-12740)
It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input when processed by tcpprep. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2020-24265, CVE-2020-24266)
It was discovered that Tcpreplay incorrectly handled certain specially crafted packet capture input when processed by tcprewrite. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 ESM. (CVE-2022-27416)
It was discovered that Tcpreplay did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted packet capture file, a remote attacker could possibly use this issue to cause Tcpreplay crash, resulting in a denial of service, or possibly read sensitive data. This issue only affected Ubuntu 18.04 ESM, Ubuntu 20.04 ESM and Ubuntu 22.04 ESM. (CVE-2022-28487)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5205-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5205.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5205-1`
`cve: CVE-2018-13112`
`cve: CVE-2018-17580`
`cve: CVE-2018-17582`
`cve: CVE-2018-17974`
`cve: CVE-2018-18407`
`cve: CVE-2018-18408`
`cve: CVE-2018-20552`
`cve: CVE-2018-20553`

... continues on next page ...

... continued from previous page ...

cve: CVE-2020-12740
cve: CVE-2020-24265
cve: CVE-2020-24266
cve: CVE-2022-27416
cve: CVE-2022-28487
advisory_id: USN-5205-1
dfn-cert: DFN-CERT-2022-1893
dfn-cert: DFN-CERT-2020-2297
dfn-cert: DFN-CERT-2020-1272
dfn-cert: DFN-CERT-2019-0003

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5880-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5880-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-110.0+build3-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Christian Holler discovered that Firefox did not properly manage memory when using PKCS 12 Safe Bag attributes. An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes. (CVE-2023-0767)
Johan Carlsson discovered that Firefox did not properly manage child iframe's unredacted URI when using Content-Security-Policy-Report-Only header. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-25728)
Vitor Torres discovered that Firefox did not properly manage permissions of extensions interaction via ExpandedPrincipals. An attacker could potentially exploits this issue to download malicious files or execute arbitrary code. (CVE-2023-25729)
Irvan Kurniawan discovered that Firefox did not properly validate background script invoking requestFullscreen. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-25730)

... continues on next page ...

... continued from previous page ...

Ronald Crane discovered that Firefox did not properly manage memory when using EncodeInputStream in xpcom. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25732)
Samuel Grob discovered that Firefox did not properly manage memory when using wrappers wrapping a scripted proxy. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25735)
Holger Fuhrmannek discovered that Firefox did not properly manage memory when using Module load requests. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25739)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25731, CVE-2023-25733, CVE-2023-25736, CVE-2023-25737, CVE-2023-25741, CVE-2023-25742, CVE-2023-25744, CVE-2023-25745)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5880-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5880.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5880-1`
`cve: CVE-2023-0767`
`cve: CVE-2023-25728`
`cve: CVE-2023-25729`
`cve: CVE-2023-25730`
`cve: CVE-2023-25731`
`cve: CVE-2023-25732`
`cve: CVE-2023-25733`
`cve: CVE-2023-25735`
`cve: CVE-2023-25736`
`cve: CVE-2023-25737`
`cve: CVE-2023-25739`
`cve: CVE-2023-25741`
`cve: CVE-2023-25742`
`cve: CVE-2023-25744`
`cve: CVE-2023-25745`
`advisory_id: USN-5880-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0407`
`cert-bund: WID-SEC-2023-0385`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0843`

... continues on next page ...

... continued from previous page ...

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

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5880-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5880-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-110.0.1+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
USN-5880-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Christian Holler discovered that Firefox did not properly manage memory when using PKCS 12 Safe Bag attributes. An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes. (CVE-2023-0767)
Johan Carlsson discovered that Firefox did not properly manage child iframe's unredacted URI when using Content-Security-Policy-Report-Only header. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-25728)
Vitor Torres discovered that Firefox did not properly manage permissions of extensions interaction via ExpandedPrincipals. An attacker could potentially exploits this issue to download malicious files or execute arbitrary code. (CVE-2023-25729)
Irvan Kurniawan discovered that Firefox did not properly validate background script invoking requestFullscreen. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-25730)

... continues on next page ...

... continued from previous page ...

Ronald Crane discovered that Firefox did not properly manage memory when using EncodeInputStream in xpcom. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25732)
Samuel Grob discovered that Firefox did not properly manage memory when using wrappers wrapping a scripted proxy. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25735)
Holger Fuhrmannek discovered that Firefox did not properly manage memory when using Module load requests. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25739)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25731, CVE-2023-25733, CVE-2023-25736, CVE-2023-25737, CVE-2023-25741, CVE-2023-25742, CVE-2023-25744, CVE-2023-25745)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5880-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5880.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5880-2`
`url: https://launchpad.net/bugs/2008861`
`cve: CVE-2023-0767`
`cve: CVE-2023-25728`
`cve: CVE-2023-25729`
`cve: CVE-2023-25730`
`cve: CVE-2023-25731`
`cve: CVE-2023-25732`
`cve: CVE-2023-25733`
`cve: CVE-2023-25735`
`cve: CVE-2023-25736`
`cve: CVE-2023-25737`
`cve: CVE-2023-25739`
`cve: CVE-2023-25741`
`cve: CVE-2023-25742`
`cve: CVE-2023-25744`
`cve: CVE-2023-25745`
`advisory_id: USN-5880-2`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0407`
`cert-bund: WID-SEC-2023-0385`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-0884`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0843
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

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5936-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5936-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: samba
Installed version: samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version: >=samba-2:4.15.13+dfsg-0ubuntu0.20.04.1

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04.

Vulnerability Insight
Evgeny Legerov discovered that Samba incorrectly handled buffers in certain GSSAPI routines of Heimdal. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-3437)
Tom Tervoort discovered that Samba incorrectly used weak rc4-hmac Kerberos keys. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-37966, CVE-2022-37967)
It was discovered that Samba supported weak RC4/HMAC-MD5 in NetLogon Secure Channel. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-38023)
Greg Hudson discovered that Samba incorrectly handled PAC parsing. On 32-bit systems, a remote attacker could use this issue to escalate privileges, or possibly execute arbitrary code. (CVE-2022-42898)
Joseph Sutton discovered that Samba could be forced to issue rc4-hmac encrypted Kerberos tickets. A remote attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-45141)
WARNING: This update upgrades the version of Samba to 4.15.13. Please see the upstreamlink moved to refer release notes for important changes in the new version:link moved to references>

... continues on next page ...

... continued from previous page ...

In addition, the security fixes included in this new version introduce several important behaviorlink moved to refer changes which may cause compatibility problems interacting with systems still expecting the former behavior. Please see the following upstream advisories for more information:link moved to references>
[link moved to references] [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5936-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5936.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5936-1`
`url: https://www.samba.org/samba/history/samba-4.15.0.html`
`url: https://www.samba.org/samba/security/CVE-2022-37966.html`
`url: https://www.samba.org/samba/security/CVE-2022-37967.html`
`url: https://www.samba.org/samba/security/CVE-2022-38023.html`
`cve: CVE-2022-3437`
`cve: CVE-2022-37966`
`cve: CVE-2022-37967`
`cve: CVE-2022-38023`
`cve: CVE-2022-42898`
`cve: CVE-2022-45141`
`advisory_id: USN-5936-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2690`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1021`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-2365`
`cert-bund: WID-SEC-2022-2057`
`cert-bund: WID-SEC-2022-1983`
`cert-bund: WID-SEC-2022-1847`
`dfn-cert: DFN-CERT-2024-1065`
`dfn-cert: DFN-CERT-2024-0839`
`dfn-cert: DFN-CERT-2023-2536`
`dfn-cert: DFN-CERT-2023-1592`
`dfn-cert: DFN-CERT-2023-1311`
`dfn-cert: DFN-CERT-2023-1230`
`dfn-cert: DFN-CERT-2023-1162`
`dfn-cert: DFN-CERT-2023-0286`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0201
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0176
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2870
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2657
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2022-2579
dfn-cert: DFN-CERT-2022-2429
dfn-cert: DFN-CERT-2022-2374
dfn-cert: DFN-CERT-2022-2364
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5822-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5822-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:    samba
Installed version:     samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.17~dfsg-0ubuntu1.20.04.5
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-5822-1 fixed vulnerabilities in Samba. The update for Ubuntu 20.04 LTS introduced regressions in certain environments. Pending investigation of these regressions, this update temporarily reverts the security fixes.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Samba incorrectly handled the bad password count logic. A remote attacker could possibly use this issue to bypass bad passwords lockouts. This issue was only addressed in Ubuntu 22.10. (CVE-2021-20251)

... continues on next page ...

... continued from previous page ...

Evgeny Legerov discovered that Samba incorrectly handled buffers in certain GSSAPI routines of Heimdal. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-3437)
Tom Tervoort discovered that Samba incorrectly used weak rc4-hmac Kerberos keys. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-37966, CVE-2022-37967)
It was discovered that Samba supported weak RC4/HMAC-MD5 in NetLogon Secure Channel. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-38023)
Greg Hudson discovered that Samba incorrectly handled PAC parsing. On 32-bit systems, a remote attacker could use this issue to escalate privileges, or possibly execute arbitrary code. (CVE-2022-42898)
Joseph Sutton discovered that Samba could be forced to issue rc4-hmac encrypted Kerberos tickets. A remote attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-45141)
WARNING: The fixes included in these updates introduce several important behavior changeslink moved to refer which may cause compatibility problems interacting with systems still expecting the former behavior. Please see the following upstream advisories for more information:link moved to references>
[link moved to references] [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5822-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5822.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5822-2`
`url: https://www.samba.org/samba/security/CVE-2022-37966.html`
`url: https://www.samba.org/samba/security/CVE-2022-37967.html`
`url: https://www.samba.org/samba/security/CVE-2022-38023.html`
`url: https://launchpad.net/bugs/2003867`
`url: https://launchpad.net/bugs/2003891`
`cve: CVE-2021-20251`
`cve: CVE-2022-3437`
`cve: CVE-2022-37966`
`cve: CVE-2022-37967`
`cve: CVE-2022-38023`
`cve: CVE-2022-42898`
`cve: CVE-2022-45141`
`advisory_id: USN-5822-2`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2690`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2023-1542`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2365
cert-bund: WID-SEC-2022-2057
cert-bund: WID-SEC-2022-1983
cert-bund: WID-SEC-2022-1847
cert-bund: WID-SEC-2022-1799
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0286
dfn-cert: DFN-CERT-2023-0201
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0176
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2870
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2657
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2022-2579
dfn-cert: DFN-CERT-2022-2429
dfn-cert: DFN-CERT-2022-2374
dfn-cert: DFN-CERT-2022-2364

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5822-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5822-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: samba
Installed version: samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version: >=samba-2:4.13.17~dfsg-0ubuntu1.20.04.4

Solution:

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
It was discovered that Samba incorrectly handled the bad password count logic. A remote attacker could possibly use this issue to bypass bad passwords lockouts. This issue was only addressed in Ubuntu 22.10. (CVE-2021-20251)
Evgeny Legerov discovered that Samba incorrectly handled buffers in certain GSSAPI routines of Heimdal. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-3437)
Tom Tervoort discovered that Samba incorrectly used weak rc4-hmac Kerberos keys. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-37966, CVE-2022-37967)
It was discovered that Samba supported weak RC4/HMAC-MD5 in NetLogon Secure Channel. A remote attacker could possibly use this issue to elevate privileges. (CVE-2022-38023)
Greg Hudson discovered that Samba incorrectly handled PAC parsing. On 32-bit systems, a remote attacker could use this issue to escalate privileges, or possibly execute arbitrary code. (CVE-2022-42898)
Joseph Sutton discovered that Samba could be forced to issue rc4-hmac encrypted Kerberos tickets. A remote attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-45141)
WARNING: The fixes included in these updates introduce several important behavior changeslink moved to refer which may cause compatibility problems interacting with systems still expecting the former behavior. Please see the following upstream advisories for more information:link moved to references>
[link moved to references] [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5822-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5822.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5822-1`
`url: https://www.samba.org/samba/security/CVE-2022-37966.html`
`url: https://www.samba.org/samba/security/CVE-2022-37967.html`
`url: https://www.samba.org/samba/security/CVE-2022-38023.html`
`cve: CVE-2021-20251`
`cve: CVE-2022-3437`
`cve: CVE-2022-37966`
`cve: CVE-2022-37967`
`cve: CVE-2022-38023`
`cve: CVE-2022-42898`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-45141
advisory_id: USN-5822-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2365
cert-bund: WID-SEC-2022-2057
cert-bund: WID-SEC-2022-1983
cert-bund: WID-SEC-2022-1847
cert-bund: WID-SEC-2022-1799
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0286
dfn-cert: DFN-CERT-2023-0201
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0176
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2870
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2657
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2022-2579
dfn-cert: DFN-CERT-2022-2429
dfn-cert: DFN-CERT-2022-2374
dfn-cert: DFN-CERT-2022-2364
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5573-1)

Summary
The remote host is missing an update for the 'rsync' package(s) announced via the USN-5573-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: rsync
Installed version: rsync-3.1.3-8
Fixed version: >=rsync-3.1.3-8ubuntu0.4

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

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

Vulnerability Insight
Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause rsync to crash, resulting in 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-5573-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5573.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5573-1
cve: CVE-2022-37434
advisory_id: USN-5573-1
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-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
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

... continues on next page ...

... continued from previous page ...

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-2022-1438
cert-bund: WID-SEC-2022-0929
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-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799
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-2022-1841
dfn-cert: DFN-CERT-2022-1710

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6074-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6074-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-113.0+build2-0ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-32216)
Irvan Kurniawan discovered that Firefox did not properly manage memory when using RLBox Expat driver. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)
Anne van Kesteren discovered that Firefox did not properly validate the import() call in service workers. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-32208)
Sam Ezeh discovered that Firefox did not properly handle certain favicon image files. If a user were tricked into opening a malicicous favicon file, an attacker could cause a denial of service. (CVE-2023-32209)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6074-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6074.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6074-1`
`cve: CVE-2023-32205`
`cve: CVE-2023-32206`
`cve: CVE-2023-32207`
`cve: CVE-2023-32208`
`cve: CVE-2023-32209`
`cve: CVE-2023-32210`
`cve: CVE-2023-32211`
`cve: CVE-2023-32212`
`cve: CVE-2023-32213`
`cve: CVE-2023-32215`
`cve: CVE-2023-32216`
`advisory_id: USN-6074-1`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1201`
`cert-bund: WID-SEC-2023-1172`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1751
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-1090
dfn-cert: DFN-CERT-2023-1040

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6074-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6074-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-113.0.1+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
USN-6074-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-32216)
Irvan Kurniawan discovered that Firefox did not properly manage memory when using RLBox Expat driver. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)
Anne van Kesteren discovered that Firefox did not properly validate the import() call in service workers. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-32208)
Sam Ezeh discovered that Firefox did not properly handle certain favicon image files. If a user were tricked into opening a malicicous favicon file, an attacker could cause a denial of service. (CVE-2023-32209)

... 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-6074-2)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6074.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6074-2
url: https://launchpad.net/bugs/2019782
cve: CVE-2023-32205
cve: CVE-2023-32206
cve: CVE-2023-32207
cve: CVE-2023-32208
cve: CVE-2023-32209
cve: CVE-2023-32210
cve: CVE-2023-32211
cve: CVE-2023-32212
cve: CVE-2023-32213
cve: CVE-2023-32215
cve: CVE-2023-32216
advisory_id: USN-6074-2
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1201
cert-bund: WID-SEC-2023-1172
dfn-cert: DFN-CERT-2023-1751
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-1090
dfn-cert: DFN-CERT-2023-1040

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6074-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6074-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-113.0.2+build1-0ubuntu0.20.04.1

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
USN-6074-1 fixed vulnerabilities and USN-6074-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-32216)
Irvan Kurniawan discovered that Firefox did not properly manage memory when using RLBox Expat driver. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)
Anne van Kesteren discovered that Firefox did not properly validate the import() call in service workers. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-32208)
Sam Ezeh discovered that Firefox did not properly handle certain favicon image files. If a user were tricked into opening a malicicous favicon file, an attacker could cause a denial of service. (CVE-2023-32209)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6074-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6074.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6074-3`
`url: https://launchpad.net/bugs/2020649`
`cve: CVE-2023-32205`
`cve: CVE-2023-32206`
`cve: CVE-2023-32207`
`cve: CVE-2023-32208`
`cve: CVE-2023-32209`
`cve: CVE-2023-32210`
`cve: CVE-2023-32211`
`cve: CVE-2023-32212`
`cve: CVE-2023-32213`
`cve: CVE-2023-32215`
`cve: CVE-2023-32216`
`advisory_id: USN-6074-3`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1201
cert-bund: WID-SEC-2023-1172
dfn-cert: DFN-CERT-2023-1751
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-1090
dfn-cert: DFN-CERT-2023-1040

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6143-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6143-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-114.0+build3-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-34417)
Jun Kokatsu discovered that Firefox did not properly validate site-isolated process for a document loaded from a data: URL that was the result of a redirect, leading to an open redirect attack. An attacker could possibly use this issue to perform phishing attacks. (CVE-2023-34415)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6143-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6143.1
Version used: 2024-02-02T04:09:01Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6143-1
cve: CVE-2023-34414
cve: CVE-2023-34415
cve: CVE-2023-34416
cve: CVE-2023-34417
advisory_id: USN-6143-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1414
cert-bund: WID-SEC-2023-1385
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1564
dfn-cert: DFN-CERT-2023-1340
dfn-cert: DFN-CERT-2023-1335
dfn-cert: DFN-CERT-2023-1305
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6143-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6143-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-114.0.1+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6143-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-34417)

... continues on next page ...

... continued from previous page ...

Jun Kokatsu discovered that Firefox did not properly validate site-isolated process for a document loaded from a data: URL that was the result of a redirect, leading to an open redirect attack. An attacker could possibly use this issue to perform phishing attacks. (CVE-2023-34415)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6143-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6143.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6143-2`
`url: https://launchpad.net/bugs/2023610`
`cve: CVE-2023-34414`
`cve: CVE-2023-34415`
`cve: CVE-2023-34416`
`cve: CVE-2023-34417`
`advisory_id: USN-6143-2`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1414`
`cert-bund: WID-SEC-2023-1385`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-1564`
`dfn-cert: DFN-CERT-2023-1340`
`dfn-cert: DFN-CERT-2023-1335`
`dfn-cert: DFN-CERT-2023-1305`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6143-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6143-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-114.0.2+build1-0ubuntu0.20.04.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6143-1 fixed vulnerabilities and USN-6143-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-34417)
Jun Kokatsu discovered that Firefox did not properly validate site-isolated process for a document loaded from a data: URL that was the result of a redirect, leading to an open redirect attack. An attacker could possibly use this issue to perform phishing attacks. (CVE-2023-34415)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6143-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6143.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6143-3`
`url: https://launchpad.net/bugs/2024513`
`cve: CVE-2023-34414`
`cve: CVE-2023-34415`
`cve: CVE-2023-34416`
`cve: CVE-2023-34417`
`advisory_id: USN-6143-3`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1414`
`cert-bund: WID-SEC-2023-1385`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-1564`
`dfn-cert: DFN-CERT-2023-1340`
`dfn-cert: DFN-CERT-2023-1335`
`dfn-cert: DFN-CERT-2023-1305`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4973-2)

Summary
The remote host is missing an update for the 'python3.8' package(s) announced via the USN-4973-2 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.1
Vulnerable package:   python3.8-minimal
Installed version:    python3.8-minimal-3.8.5-1~20.04.3
Fixed version:      >=python3.8-minimal-3.8.10-0ubuntu1~20.04.1
```

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

Affected Software/OS
'python3.8' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-4973-1 fixed this vulnerability previously, but it was re-introduced in python3.8 in focal because of the SRU in LP: #1928057. This update fixes the problem.
Original advisory details:
It was discovered that the Python stdlib ipaddress API incorrectly handled octal strings. A remote attacker could possibly use this issue to perform a wide variety of attacks, including bypassing certain access restrictions.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4973-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4973.2
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-4973-2
url: https://launchpad.net/bugs/1945240
cve: CVE-2021-29921
advisory_id: USN-4973-2
cert-bund: WID-SEC-2023-2460
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-0624
cert-bund: WID-SEC-2022-0464
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2021-2354
dfn-cert: DFN-CERT-2021-2353
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1534
dfn-cert: DFN-CERT-2021-1414
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1303
dfn-cert: DFN-CERT-2021-1184
dfn-cert: DFN-CERT-2021-0956

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6267-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6267-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-116.0+build2-0ubuntu0.20.04.2

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4051, CVE-2023-4053, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4058)
Max Vlasov discovered that Firefox Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2023-4045)
Alexander Guryanov discovered that Firefox did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)
Mark Brand discovered that Firefox did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6267-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6267.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6267-1
cve: CVE-2023-4045
cve: CVE-2023-4046
cve: CVE-2023-4047
cve: CVE-2023-4048
cve: CVE-2023-4049
cve: CVE-2023-4050
cve: CVE-2023-4051
cve: CVE-2023-4053
cve: CVE-2023-4055
cve: CVE-2023-4056
cve: CVE-2023-4057
cve: CVE-2023-4058
advisory_id: USN-6267-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2202
cert-bund: WID-SEC-2023-1934
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2359
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2047
dfn-cert: DFN-CERT-2023-2028
dfn-cert: DFN-CERT-2023-2004
dfn-cert: DFN-CERT-2023-1779
dfn-cert: DFN-CERT-2023-1761

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5227-3)

Summary

The remote host is missing an update for the 'pillow' package(s) announced via the USN-5227-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: python3-pil
Installed version: python3-pil-7.0.0-4ubuntu0.4
Fixed version: >=python3-pil-7.0.0-4ubuntu0.6

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
USN-5227-1 fixed vulnerabilities in Pillow. It was discovered that the fix for CVE-2022-22817 was incomplete. This update fixes the problem.
Original advisory details:
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to hang, resulting in a denial of service. (CVE-2021-23437)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. This issue ony affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-34552)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22815)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. (CVE-2022-22816)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22817)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5227-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5227.3
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-5227-3`
`cve: CVE-2022-22817`
`advisory_id: USN-5227-3`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K22/0229`
`dfn-cert: DFN-CERT-2024-0767`
`dfn-cert: DFN-CERT-2024-0284`
`dfn-cert: DFN-CERT-2022-1142`
`dfn-cert: DFN-CERT-2022-0320`
`dfn-cert: DFN-CERT-2022-0168`
`dfn-cert: DFN-CERT-2022-0087`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5227-1)

Summary
The remote host is missing an update for the 'pillow' package(s) announced via the USN-5227-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-pil
Installed version:    python3-pil-7.0.0-4ubuntu0.4
Fixed version:      >=python3-pil-7.0.0-4ubuntu0.5
```

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

Affected Software/OS
'pillow' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to hang, resulting in a denial of service. (CVE-2021-23437)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-34552)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22815)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. (CVE-2022-22816)
It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22817)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5227-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5227.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5227-1`

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2021-23437
cve: CVE-2021-34552
cve: CVE-2022-22815
cve: CVE-2022-22816
cve: CVE-2022-22817
advisory_id: USN-5227-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2022-1835
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0229
cert-bund: CB-K21/1197
dfn-cert: DFN-CERT-2024-1344
dfn-cert: DFN-CERT-2024-1339
dfn-cert: DFN-CERT-2024-0767
dfn-cert: DFN-CERT-2024-0284
dfn-cert: DFN-CERT-2022-1142
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0168
dfn-cert: DFN-CERT-2022-0087
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2349
dfn-cert: DFN-CERT-2021-2189
dfn-cert: DFN-CERT-2021-2104
dfn-cert: DFN-CERT-2021-1930
dfn-cert: DFN-CERT-2021-1913
dfn-cert: DFN-CERT-2021-1706
dfn-cert: DFN-CERT-2021-1601
dfn-cert: DFN-CERT-2021-1583
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6517-1)

Summary
The remote host is missing an update for the 'perl' package(s) announced via the USN-6517-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   perl
Installed version:    perl-5.30.0-9ubuntu0.2
Fixed version:      >=perl-5.30.0-9ubuntu0.5
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'perl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Perl incorrectly handled printing certain warning messages. An attacker could possibly use this issue to cause Perl to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-48522)
Nathan Mills discovered that Perl incorrectly handled certain regular expressions. An attacker could use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-47038)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6517-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6517.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6517-1`
`cve: CVE-2022-48522`
`cve: CVE-2023-47038`
`advisory_id: USN-6517-1`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2023-3007`
`cert-bund: WID-SEC-2023-2113`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2024-0469`
`dfn-cert: DFN-CERT-2023-2982`
`dfn-cert: DFN-CERT-2023-2981`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5347-1)

Summary
The remote host is missing an update for the 'openvpn' package(s) announced via the USN-5347-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  openvpn`

... continues on next page ...

... continued from previous page ...

```
Installed version:    openvpn-2.4.7-1ubuntu2.20.04.2
Fixed version:      >=openvpn-2.4.7-1ubuntu2.20.04.4
```

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

Affected Software/OS
'openvpn' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that OpenVPN incorrectly handled certain configurations with multiple authentication plugins. A remote attacker could possibly use this issue to bypass authentication using incomplete credentials.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5347-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5347.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5347-1`
`cve: CVE-2022-0547`
`advisory_id: USN-5347-1`
`cert-bund: WID-SEC-2022-0116`
`dfn-cert: DFN-CERT-2022-0977`
`dfn-cert: DFN-CERT-2022-0615`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5488-1)

Summary
The remote host is missing an update for the 'openssl, openssl1.0' package(s) announced via the USN-5488-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openssl
Installed version:    openssl-1.1.1f-1ubuntu2.4
Fixed version:      >=openssl-1.1.1f-1ubuntu2.15
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'openssl, openssl1.0' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Chancen and Daniel Fiala discovered that OpenSSL incorrectly handled the c_rehash script. A local attacker could possibly use this issue to execute arbitrary commands when c_rehash is run.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5488-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5488.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5488-1`
`cve: CVE-2022-2068`
`advisory_id: USN-5488-1`
`cert-bund: WID-SEC-2024-1186`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0054`
`cert-bund: WID-SEC-2023-2723`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2022-1766`
`cert-bund: WID-SEC-2022-1461`
`cert-bund: WID-SEC-2022-1245`
`cert-bund: WID-SEC-2022-1068`
`cert-bund: WID-SEC-2022-0425`
`dfn-cert: DFN-CERT-2024-0147`
`dfn-cert: DFN-CERT-2024-0059`
`dfn-cert: DFN-CERT-2023-2667`
`dfn-cert: DFN-CERT-2023-2600`
`dfn-cert: DFN-CERT-2023-2599`
`dfn-cert: DFN-CERT-2023-2571`
`dfn-cert: DFN-CERT-2023-0100`
`dfn-cert: DFN-CERT-2022-2799`
`dfn-cert: DFN-CERT-2022-2150`
`dfn-cert: DFN-CERT-2022-2111`
`dfn-cert: DFN-CERT-2022-2073`
`dfn-cert: DFN-CERT-2022-2072`
`dfn-cert: DFN-CERT-2022-1905`
`dfn-cert: DFN-CERT-2022-1740`
`dfn-cert: DFN-CERT-2022-1646`
`dfn-cert: DFN-CERT-2022-1552`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1393

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5090-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5090-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.5
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-bin-2.4.41-4ubuntu3.5
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
James Kettle discovered that the Apache HTTP Server HTTP/2 module incorrectly handled certain crafted methods. A remote attacker could possibly use this issue to perform request splitting or cache poisoning attacks. (CVE-2021-33193)
It was discovered that the Apache HTTP Server incorrectly handled certain malformed requests. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2021-34798)
Li Zhi Xin discovered that the Apache mod_proxy_uwsgi module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-36160)
It was discovered that the Apache HTTP Server incorrectly handled escaping quotes. If the server was configured with third-party modules, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-39275)

... continues on next page ...

... continued from previous page ...

It was discovered that the Apache mod_proxy module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to forward requests to arbitrary origin servers. (CVE-2021-40438)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5090-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.5090.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5090-1`
`cve: CVE-2021-33193`
`cve: CVE-2021-34798`
`cve: CVE-2021-36160`
`cve: CVE-2021-39275`
`cve: CVE-2021-40438`
`advisory_id: USN-5090-1`
`cert-bund: WID-SEC-2024-0186`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1016`
`cert-bund: WID-SEC-2022-1298`
`cert-bund: WID-SEC-2022-1189`
`cert-bund: WID-SEC-2022-0724`
`cert-bund: WID-SEC-2022-0722`
`cert-bund: WID-SEC-2022-0190`
`cert-bund: CB-K22/0476`
`cert-bund: CB-K22/0465`
`cert-bund: CB-K22/0463`
`cert-bund: CB-K21/0992`
`cert-bund: CB-K21/0878`
`dfn-cert: DFN-CERT-2023-0881`
`dfn-cert: DFN-CERT-2023-0497`
`dfn-cert: DFN-CERT-2022-2405`
`dfn-cert: DFN-CERT-2022-2167`
`dfn-cert: DFN-CERT-2022-1047`
`dfn-cert: DFN-CERT-2022-0904`
`dfn-cert: DFN-CERT-2022-0878`
`dfn-cert: DFN-CERT-2022-0872`
`dfn-cert: DFN-CERT-2022-0869`
`dfn-cert: DFN-CERT-2022-0672`
`dfn-cert: DFN-CERT-2022-0207`
`dfn-cert: DFN-CERT-2022-0119`
`dfn-cert: DFN-CERT-2022-0098`
`dfn-cert: DFN-CERT-2021-2629`
`dfn-cert: DFN-CERT-2021-2471`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2164
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-2098
dfn-cert: DFN-CERT-2021-2090
dfn-cert: DFN-CERT-2021-2047
dfn-cert: DFN-CERT-2021-2034
dfn-cert: DFN-CERT-2021-2020
dfn-cert: DFN-CERT-2021-1961
dfn-cert: DFN-CERT-2021-1854
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5090-3)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5090-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.6
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-bin-2.4.41-4ubuntu3.6
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
USN-5090-1 fixed vulnerabilities in Apache HTTP Server. One of the upstream fixes introduced a regression in UDS URIs. This update fixes the problem.
Original advisory details:
James Kettle discovered that the Apache HTTP Server HTTP/2 module incorrectly handled certain crafted methods. A remote attacker could possibly use this issue to perform request splitting or cache poisoning attacks. (CVE-2021-33193)
It was discovered that the Apache HTTP Server incorrectly handled certain malformed requests. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2021-34798)

... continues on next page ...

... continued from previous page ...

Li Zhi Xin discovered that the Apache mod_proxy_uwsgi module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-36160)
It was discovered that the Apache HTTP Server incorrectly handled escaping quotes. If the server was configured with third-party modules, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-39275)
It was discovered that the Apache mod_proxy module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to forward requests to arbitrary origin servers. (CVE-2021-40438)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5090-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5090.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5090-3`
`url: https://launchpad.net/bugs/1945311`
`cve: CVE-2021-33193`
`cve: CVE-2021-34798`
`cve: CVE-2021-36160`
`cve: CVE-2021-39275`
`cve: CVE-2021-40438`
`advisory_id: USN-5090-3`
`cert-bund: WID-SEC-2024-0186`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1016`
`cert-bund: WID-SEC-2022-1298`
`cert-bund: WID-SEC-2022-1189`
`cert-bund: WID-SEC-2022-0724`
`cert-bund: WID-SEC-2022-0722`
`cert-bund: WID-SEC-2022-0190`
`cert-bund: CB-K22/0476`
`cert-bund: CB-K22/0465`
`cert-bund: CB-K22/0463`
`cert-bund: CB-K21/0992`
`cert-bund: CB-K21/0878`
`dfn-cert: DFN-CERT-2023-0881`
`dfn-cert: DFN-CERT-2023-0497`
`dfn-cert: DFN-CERT-2022-2405`
`dfn-cert: DFN-CERT-2022-2167`
`dfn-cert: DFN-CERT-2022-1047`
`dfn-cert: DFN-CERT-2022-0904`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0878
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0869
dfn-cert: DFN-CERT-2022-0672
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2022-0119
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2021-2629
dfn-cert: DFN-CERT-2021-2471
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-2164
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-2098
dfn-cert: DFN-CERT-2021-2090
dfn-cert: DFN-CERT-2021-2047
dfn-cert: DFN-CERT-2021-2034
dfn-cert: DFN-CERT-2021-2020
dfn-cert: DFN-CERT-2021-1961
dfn-cert: DFN-CERT-2021-1854
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5212-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5212-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.9
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-bin-2.4.41-4ubuntu3.9
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that the Apache HTTP Server incorrectly handled certain forward proxy requests. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly perform a Server Side Request Forgery attack. (CVE-2021-44224)
It was discovered that the Apache HTTP Server Lua module incorrectly handled memory in the multipart parser. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-44790)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5212-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5212.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5212-1`
`cve: CVE-2021-44224`
`cve: CVE-2021-44790`
`advisory_id: USN-5212-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1057`
`cert-bund: WID-SEC-2022-0727`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: WID-SEC-2022-0190`
`cert-bund: CB-K22/0619`
`cert-bund: CB-K21/1296`
`dfn-cert: DFN-CERT-2022-2405`
`dfn-cert: DFN-CERT-2022-2167`
`dfn-cert: DFN-CERT-2022-1116`
`dfn-cert: DFN-CERT-2022-1115`
`dfn-cert: DFN-CERT-2022-1114`
`dfn-cert: DFN-CERT-2022-1047`
`dfn-cert: DFN-CERT-2022-0872`
`dfn-cert: DFN-CERT-2022-0747`
`dfn-cert: DFN-CERT-2022-0369`
`dfn-cert: DFN-CERT-2022-0192`
`dfn-cert: DFN-CERT-2022-0098`
`dfn-cert: DFN-CERT-2022-0068`
`dfn-cert: DFN-CERT-2021-2656`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5333-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'apache2' package(s) announced via the USN-5333-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.10
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-bin-2.4.41-4ubuntu3.10
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Chamal De Silva discovered that the Apache HTTP Server mod_lua module incorrectly handled certain crafted request bodies. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2022-22719)
James Kettle discovered that the Apache HTTP Server incorrectly closed inbound connection when certain errors are encountered. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2022-22720)
It was discovered that the Apache HTTP Server incorrectly handled large LimitXMLRequestBody settings on certain platforms. In certain configurations, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-22721)
Ronald Crane discovered that the Apache HTTP Server mod_sed module incorrectly handled memory. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-23943)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5333-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5333.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5333-1
cve: CVE-2022-22719
cve: CVE-2022-22720
cve: CVE-2022-22721
```

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-23943
advisory_id: USN-5333-1
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0898
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0646
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0290
cert-bund: CB-K22/0619
cert-bund: CB-K22/0306
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2509
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0747
dfn-cert: DFN-CERT-2022-0678
dfn-cert: DFN-CERT-2022-0582
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6560-1)

Summary
The remote host is missing an update for the 'openssh' package(s) announced via the USN-6560-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openssh-client
Installed version:    openssh-client-1:8.2p1-4ubuntu0.2
Fixed version:      >=openssh-client-1:8.2p1-4ubuntu0.10
Vulnerable package:   openssh-server
Installed version:    openssh-server-1:8.2p1-4ubuntu0.2
Fixed version:      >=openssh-server-1:8.2p1-4ubuntu0.10
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'openssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Fabian Baumer, Marcus Brinkmann, Jorg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue. (CVE-2023-48795)
Luci Stanescu discovered that OpenSSH incorrectly added destination constraints when smartcard keys were added to ssh-agent, contrary to expectations. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-28531)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6560-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6560.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6560-1`
`cve: CVE-2023-28531`
`cve: CVE-2023-48795`
`advisory_id: USN-6560-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1228`
`cert-bund: WID-SEC-2024-1186`
`cert-bund: WID-SEC-2024-1082`
`cert-bund: WID-SEC-2024-0899`
`cert-bund: WID-SEC-2024-0892`
`cert-bund: WID-SEC-2024-0889`
`cert-bund: WID-SEC-2024-0885`
`cert-bund: WID-SEC-2024-0874`
`cert-bund: WID-SEC-2024-0869`
`cert-bund: WID-SEC-2024-0578`
`cert-bund: WID-SEC-2024-0564`
`cert-bund: WID-SEC-2024-0523`
`cert-bund: WID-SEC-2023-3174`
`cert-bund: WID-SEC-2023-0670`
`dfn-cert: DFN-CERT-2024-1443`
`dfn-cert: DFN-CERT-2024-1442`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0341
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0013

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175
dfn-cert: DFN-CERT-2023-1424
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5570-2)

Summary
The remote host is missing an update for the 'zlib' package(s) announced via the USN-5570-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   zlib1g
Installed version:    zlib1g-1:1.2.11.dfsg-2ubuntu1.2
Fixed version:      >=zlib1g-1:1.2.11.dfsg-2ubuntu1.5
```

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

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

Vulnerability Insight
USN-5570-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 22.04 LTS and Ubuntu 20.04 LTS.
Original advisory details:
Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5570-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5570.2
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5570-2
cve: CVE-2022-37434
advisory_id: USN-5570-2
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-2023-1812
cert-bund: WID-SEC-2023-1791
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
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-2023-0140
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-2022-1438
cert-bund: WID-SEC-2022-0929
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-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2799

... continues on next page ...

... continued from previous page ...

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-2022-1841
dfn-cert: DFN-CERT-2022-1710

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6242-1)

Summary
The remote host is missing an update for the 'openssh' package(s) announced via the USN-6242-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: openssh-client
Installed version: openssh-client-1:8.2p1-4ubuntu0.2
Fixed version: >=openssh-client-1:8.2p1-4ubuntu0.8

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

Affected Software/OS
'openssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that OpenSSH incorrectly handled loading certain PKCS#11 providers. If a user forwarded their ssh-agent to an untrusted system, a remote attacker could possibly use this issue to load arbitrary libraries from the user's system and execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6242-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6242.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6242-1
cve: CVE-2023-38408

... continues on next page ...

... continued from previous page ...

```
advisory_id: USN-6242-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1082
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2240
cert-bund: WID-SEC-2023-1843
cert-bund: WID-SEC-2023-1819
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-1961
dfn-cert: DFN-CERT-2023-1920
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1773
dfn-cert: DFN-CERT-2023-1665
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6548-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-xilinx-zynqmp' package(s) announced via the USN-6548-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.169.167
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that Spectre-BHB mitigations were missing for Ampere processors. A local attacker could potentially use this to expose sensitive information. (CVE-2023-3006)
It was discovered that the USB subsystem in the Linux kernel contained a race condition while handling device descriptors in certain situations, leading to a out-of-bounds read vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-37453)
Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate some attributes passed from userspace. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2023-39189)
Sunjoo Park discovered that the netfilter subsystem in the Linux kernel did not properly validate u32 packets content, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39192)
Lucas Leong discovered that the netfilter subsystem in the Linux kernel did not properly validate SCTP data, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39193)
Lucas Leong discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel did not properly handle state filters, leading to an out- of-bounds read vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-39194)
Kyle Zeng discovered that the IPv4 implementation in the Linux kernel did not properly handle socket buffers (skb) when performing IP routing in certain circumstances, leading to a null pointer dereference vulnerability. A privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-42754)
Alon Zahavi discovered that the NVMe-oF/TCP subsystem in the Linux kernel did not properly handle queue initialization failures in certain situations, 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-2023-5178)
Budimir Markovic discovered that the perf subsystem in the Linux kernel did not properly handle event groups, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-5717)
It was discovered that the TLS subsystem in the Linux kernel did not properly perform cryptographic operations in some situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6176)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6548-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6548.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6548-1`
`cve: CVE-2023-3006`
`cve: CVE-2023-37453`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2023-39189
cve: CVE-2023-39192
cve: CVE-2023-39193
cve: CVE-2023-39194
cve: CVE-2023-42754
cve: CVE-2023-5178
cve: CVE-2023-5717
cve: CVE-2023-6176
advisory_id: USN-6548-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2023-2950
cert-bund: WID-SEC-2023-2746
cert-bund: WID-SEC-2023-2649
cert-bund: WID-SEC-2023-2598
cert-bund: WID-SEC-2023-2553
cert-bund: WID-SEC-2023-2530
cert-bund: WID-SEC-2023-2525
cert-bund: WID-SEC-2023-1680
cert-bund: WID-SEC-2023-1339
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1212
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1068
dfn-cert: DFN-CERT-2024-1056
dfn-cert: DFN-CERT-2024-1055
dfn-cert: DFN-CERT-2024-0925
dfn-cert: DFN-CERT-2024-0863
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0730
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0654
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0487
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0452
dfn-cert: DFN-CERT-2024-0396
dfn-cert: DFN-CERT-2024-0351
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0325
dfn-cert: DFN-CERT-2024-0321
dfn-cert: DFN-CERT-2024-0320
dfn-cert: DFN-CERT-2024-0308
dfn-cert: DFN-CERT-2024-0307
dfn-cert: DFN-CERT-2024-0280
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0266
dfn-cert: DFN-CERT-2024-0260
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0248
dfn-cert: DFN-CERT-2024-0247
dfn-cert: DFN-CERT-2024-0213
dfn-cert: DFN-CERT-2024-0201
dfn-cert: DFN-CERT-2024-0198
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2024-0095
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0015
dfn-cert: DFN-CERT-2023-3148
dfn-cert: DFN-CERT-2023-3147
dfn-cert: DFN-CERT-2023-3123
dfn-cert: DFN-CERT-2023-3121
dfn-cert: DFN-CERT-2023-3120
dfn-cert: DFN-CERT-2023-3114
dfn-cert: DFN-CERT-2023-3113
dfn-cert: DFN-CERT-2023-3085
dfn-cert: DFN-CERT-2023-3084
dfn-cert: DFN-CERT-2023-3055
dfn-cert: DFN-CERT-2023-3054
dfn-cert: DFN-CERT-2023-3053
dfn-cert: DFN-CERT-2023-3046
dfn-cert: DFN-CERT-2023-3045
dfn-cert: DFN-CERT-2023-2989
dfn-cert: DFN-CERT-2023-2985
dfn-cert: DFN-CERT-2023-2984
dfn-cert: DFN-CERT-2023-2944
dfn-cert: DFN-CERT-2023-2932
dfn-cert: DFN-CERT-2023-2923
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2800
dfn-cert: DFN-CERT-2023-2745
dfn-cert: DFN-CERT-2023-2744
dfn-cert: DFN-CERT-2023-2743
dfn-cert: DFN-CERT-2023-2725
dfn-cert: DFN-CERT-2023-2723
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2721
dfn-cert: DFN-CERT-2023-2720
dfn-cert: DFN-CERT-2023-2719
dfn-cert: DFN-CERT-2023-2718
dfn-cert: DFN-CERT-2023-2683

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2507
dfn-cert: DFN-CERT-2023-2506
dfn-cert: DFN-CERT-2023-2497
dfn-cert: DFN-CERT-2023-2496
dfn-cert: DFN-CERT-2023-2466
dfn-cert: DFN-CERT-2023-2465
dfn-cert: DFN-CERT-2023-2464
dfn-cert: DFN-CERT-2023-2426
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2389
dfn-cert: DFN-CERT-2023-2162
dfn-cert: DFN-CERT-2023-2161
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1370

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5475-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5475-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-101.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the browser UI, conduct cross-site scripting (XSS) attacks, bypass content security policy (CSP) restrictions, or execute arbitrary code.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5475-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5475.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5475-1
cve: CVE-2022-1919
cve: CVE-2022-31736
cve: CVE-2022-31737
cve: CVE-2022-31738
cve: CVE-2022-31740
cve: CVE-2022-31741
cve: CVE-2022-31742
cve: CVE-2022-31743
cve: CVE-2022-31744
cve: CVE-2022-31745
cve: CVE-2022-31747
cve: CVE-2022-31748
advisory_id: USN-5475-1
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0019
cert-bund: CB-K22/0671
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1535
dfn-cert: DFN-CERT-2022-1441
dfn-cert: DFN-CERT-2022-1440
dfn-cert: DFN-CERT-2022-1430
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1303
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1231
dfn-cert: DFN-CERT-2022-1230

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5536-1)

Summary

The remote host is missing an update for the 'firefox' package(s) announced via the USN-5536-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-103.0+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the mouse pointer position, bypass Subresource Integrity protections, obtain sensitive information, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5536-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5536.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5536-1
cve: CVE-2022-2505
cve: CVE-2022-36315
cve: CVE-2022-36316
cve: CVE-2022-36318
cve: CVE-2022-36319
cve: CVE-2022-36320
advisory_id: USN-5536-1
cert-bund: WID-SEC-2022-0859
cert-bund: WID-SEC-2022-0837
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2225
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1679
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1654

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5512-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5512-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:91.11.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass CSP restrictions, or execute arbitrary code. (CVE-2022-2200, CVE-2022-31736, CVE-2022-31737, CVE-2022-31738, CVE-2022-31740, CVE-2022-31741, CVE-2022-31742, CVE-2022-31744, CVE-2022-31747, CVE-2022-34468, CVE-2022-34470, CVE-2022-34479, CVE-2022-34481, CVE-2022-34484)
It was discovered that an unavailable PAC file caused OCSP requests to be blocked, resulting in incorrect error pages being displayed. (CVE-2022-34472)
It was discovered that the Braille space character could be used to cause Thunderbird to display the wrong sender address for signed messages. An attacker could potentially exploit this to trick the user into believing a message had been sent from somebody they trusted. (CVE-2022-1834)
It was discovered that Thunderbird would consider an email with a mismatched OpenPGP signature date as valid. An attacker could potentially exploit this by replaying an older message in order to trick the user into believing that the statements in the message are current. (CVE-2022-2226)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5512-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5512.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5512-1
cve: CVE-2022-1834
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2022-2200
cve: CVE-2022-2226
cve: CVE-2022-31736
cve: CVE-2022-31737
cve: CVE-2022-31738
cve: CVE-2022-31740
cve: CVE-2022-31741
cve: CVE-2022-31742
cve: CVE-2022-31744
cve: CVE-2022-31747
cve: CVE-2022-34468
cve: CVE-2022-34470
cve: CVE-2022-34472
cve: CVE-2022-34479
cve: CVE-2022-34481
cve: CVE-2022-34484
advisory_id: USN-5512-1
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0505
cert-bund: WID-SEC-2022-0019
cert-bund: CB-K22/0671
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1535
dfn-cert: DFN-CERT-2022-1441
dfn-cert: DFN-CERT-2022-1440
dfn-cert: DFN-CERT-2022-1430
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1303
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1231
dfn-cert: DFN-CERT-2022-1230
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5435-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5435-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:91.9.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass permission prompts, obtain sensitive information, bypass security restrictions, cause user confusion, or execute arbitrary code. (CVE-2022-29909, CVE-2022-29911, CVE-2022-29912, CVE-2022-29913, CVE-2022-29914, CVE-2022-29916, CVE-2022-29917)
It was discovered that Thunderbird would show the wrong security status after viewing an attached message that is signed or encrypted. An attacker could potentially exploit this by tricking the user into trusting the authenticity of a message. (CVE-2022-1520)
It was discovered that the methods of an Array object could be corrupted as a result of prototype pollution by sending a message to the parent process. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could exploit this to execute JavaScript in a privileged context. (CVE-2022-1529, CVE-2022-1802)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5435-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5435.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5435-1
cve: CVE-2022-1520
cve: CVE-2022-1529
cve: CVE-2022-1802
cve: CVE-2022-29909
cve: CVE-2022-29911
cve: CVE-2022-29912
cve: CVE-2022-29913
cve: CVE-2022-29914
cve: CVE-2022-29916
cve: CVE-2022-29917
advisory_id: USN-5435-1

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0538
cert-bund: WID-SEC-2022-0537
cert-bund: WID-SEC-2022-0129
cert-bund: CB-K22/0642
cert-bund: CB-K22/0542
cert-bund: CB-K22/0534
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
dfn-cert: DFN-CERT-2022-1162
dfn-cert: DFN-CERT-2022-1007
dfn-cert: DFN-CERT-2022-1003
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0978

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5487-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5487-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: apache2
Installed version: apache2-2.4.41-4ubuntu3.3
Fixed version: >=apache2-2.4.41-4ubuntu3.12
Vulnerable package: apache2-bin
Installed version: apache2-bin-2.4.41-4ubuntu3.3
Fixed version: >=apache2-bin-2.4.41-4ubuntu3.12

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

Affected Software/OS
'apache2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that Apache HTTP Server mod_proxy_ajp incorrectly handled certain crafted request. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2022-26377)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-28614)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash or expose sensitive information. (CVE-2022-28615)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-29404)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash. (CVE-2022-30522)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2022-30556)
It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to bypass IP based authentication. (CVE-2022-31813)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5487-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5487.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5487-1`
`cve: CVE-2022-26377`
`cve: CVE-2022-28614`
`cve: CVE-2022-28615`
`cve: CVE-2022-29404`
`cve: CVE-2022-30522`
`cve: CVE-2022-30556`
`cve: CVE-2022-31813`
`advisory_id: USN-5487-1`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-0134`
`cert-bund: WID-SEC-2023-0132`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1766`
`cert-bund: WID-SEC-2022-1764`
`cert-bund: WID-SEC-2022-0858`
`cert-bund: WID-SEC-2022-0192`
`cert-bund: CB-K22/0692`
`dfn-cert: DFN-CERT-2023-0119`
`dfn-cert: DFN-CERT-2022-2799`
`dfn-cert: DFN-CERT-2022-2789`
`dfn-cert: DFN-CERT-2022-2652`
`dfn-cert: DFN-CERT-2022-2509`
`dfn-cert: DFN-CERT-2022-2310`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1833
dfn-cert: DFN-CERT-2022-1720
dfn-cert: DFN-CERT-2022-1353
dfn-cert: DFN-CERT-2022-1296

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5446-1)

Summary
The remote host is missing an update for the 'dpkg' package(s) announced via the USN-5446-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   dpkg
Installed version:    dpkg-1.19.7ubuntu3
Fixed version:      >=dpkg-1.19.7ubuntu3.2
Vulnerable package:   libdpkg-perl
Installed version:    libdpkg-perl-1.19.7ubuntu3
Fixed version:      >=libdpkg-perl-1.19.7ubuntu3.2
```

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

Affected Software/OS
'dpkg' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Max Justicz discovered that dpkg incorrectly handled unpacking certain source packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could modify files outside the target unpack directory, leading to a denial of service or potentially gaining access to the system.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5446-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5446.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5446-1`

... continues on next page ...

. . . continued from previous page . . .

cve: CVE-2022-1664
advisory_id: USN-5446-1
cert-bund: WID-SEC-2022-0932
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1194

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6404-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6404-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-118.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172, CVE-2023-5175, CVE-2023-5176)
Ronald Crane discovered that Firefox did not properly manage memory when non-HTTPS Alternate Services (network.http.altsvc.oe) is enabled. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5173)
Clement Lecigne discovered that Firefox did not properly manage memory when handling VP8 media stream. An attacker-controlled VP8 media stream could lead to a heap buffer overflow in the content process, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-5217)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6404-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6404.1

. . . continues on next page . . .

... continued from previous page ...

Version used: 2024-02-01T08:21:47Z

References

url: https://ubuntu.com/security/notices/USN-6404-1
cve: CVE-2023-5169
cve: CVE-2023-5170
cve: CVE-2023-5171
cve: CVE-2023-5172
cve: CVE-2023-5173
cve: CVE-2023-5175
cve: CVE-2023-5176
cve: CVE-2023-5217
advisory_id: USN-6404-1
cert-bund: WID-SEC-2023-2599
cert-bund: WID-SEC-2023-2572
cert-bund: WID-SEC-2023-2514
cert-bund: WID-SEC-2023-2498
cert-bund: WID-SEC-2023-2448
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2484
dfn-cert: DFN-CERT-2023-2435
dfn-cert: DFN-CERT-2023-2433
dfn-cert: DFN-CERT-2023-2397
dfn-cert: DFN-CERT-2023-2395
dfn-cert: DFN-CERT-2023-2384
dfn-cert: DFN-CERT-2023-2377
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2357
dfn-cert: DFN-CERT-2023-2348
dfn-cert: DFN-CERT-2023-2344
dfn-cert: DFN-CERT-2023-2330
dfn-cert: DFN-CERT-2023-2310
dfn-cert: DFN-CERT-2023-2285
dfn-cert: DFN-CERT-2023-2281

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6420-1)

Summary

The remote host is missing an update for the 'vim' package(s) announced via the USN-6420-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.18
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.18
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.18
```

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

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

Vulnerability Insight
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3235, CVE-2022-3278, CVE-2022-3297, CVE-2022-3491)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3352, CVE-2022-4292)
It was discovered that Vim incorrectly handled memory when replacing in virtualedit mode. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3234)
It was discovered that Vim incorrectly handled memory when autocmd changes mark. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3256)
It was discovered that Vim did not properly perform checks on array index with negative width window. An attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2022-3324)
It was discovered that Vim did not properly perform checks on a put command column with a visual block. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3520)
It was discovered that Vim incorrectly handled memory when using autocommand to open a window. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3591)
It was discovered that Vim incorrectly handled memory when updating buffer of the component autocmd handler. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3705)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim incorrectly handled floating point comparison with incorrect operator. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS. and Ubuntu 22.04 LTS. (CVE-2022-4293)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6420-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6420.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-6420-1`
`cve: CVE-2022-3234`
`cve: CVE-2022-3235`
`cve: CVE-2022-3256`
`cve: CVE-2022-3278`
`cve: CVE-2022-3297`
`cve: CVE-2022-3324`
`cve: CVE-2022-3352`
`cve: CVE-2022-3491`
`cve: CVE-2022-3520`
`cve: CVE-2022-3591`
`cve: CVE-2022-3705`
`cve: CVE-2022-4292`
`cve: CVE-2022-4293`
`advisory_id: USN-6420-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0189`
`cert-bund: WID-SEC-2022-2248`
`cert-bund: WID-SEC-2022-2238`
`cert-bund: WID-SEC-2022-2222`
`cert-bund: WID-SEC-2022-1876`
`cert-bund: WID-SEC-2022-1584`
`cert-bund: WID-SEC-2022-1540`
`cert-bund: WID-SEC-2022-1532`
`cert-bund: WID-SEC-2022-1503`
`cert-bund: WID-SEC-2022-1457`
`dfn-cert: DFN-CERT-2023-2428`
`dfn-cert: DFN-CERT-2023-0237`
`dfn-cert: DFN-CERT-2023-0230`
`dfn-cert: DFN-CERT-2023-0156`
`dfn-cert: DFN-CERT-2022-2929`
`dfn-cert: DFN-CERT-2022-2921`
`dfn-cert: DFN-CERT-2022-2819`
`dfn-cert: DFN-CERT-2022-2716`
`dfn-cert: DFN-CERT-2022-2675`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-2473
dfn-cert: DFN-CERT-2022-2257

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6026-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6026-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vim
Installed version: vim-2:8.1.2269-1ubuntu5
Fixed version: >=vim-2:8.1.2269-1ubuntu5.14

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

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

Vulnerability Insight
It was discovered that Vim was incorrectly processing Vim buffers. An attacker could possibly use this issue to perform illegal memory access and expose sensitive information. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-4166)
It was discovered that Vim was using freed memory when dealing with regular expressions inside a visual selection. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-4192)
It was discovered that Vim was incorrectly handling virtual column position operations, which could result in an out-of-bounds read. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-4193)
It was discovered that Vim was not properly performing bounds checks when updating windows present on a screen, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0213)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim was incorrectly performing read and write operations when in visual block mode, going beyond the end of a line and causing a heap buffer overflow. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-0261, CVE-2022-0318)
It was discovered that Vim was incorrectly handling window exchanging operations when in Visual mode, which could result in an out-of-bounds read. An attacker could possibly use this issue to expose sensitive information. (CVE-2022-0319)
It was discovered that Vim was incorrectly handling recursion when parsing conditional expressions. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0351)
It was discovered that Vim was not properly handling memory allocation when processing data in Ex mode, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0359)
It was discovered that Vim was not properly performing bounds checks when executing line operations in Visual mode, which could result in a heap buffer overflow. 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 and Ubuntu 22.04 LTS. (CVE-2022-0361, CVE-2022-0368)
It was discovered that Vim was not properly handling loop conditions when looking for spell suggestions, which could result in a ... [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-6026-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6026.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6026-1`
`cve: CVE-2021-4166`
`cve: CVE-2021-4192`
`cve: CVE-2021-4193`
`cve: CVE-2022-0213`
`cve: CVE-2022-0261`
`cve: CVE-2022-0318`
`cve: CVE-2022-0319`
`cve: CVE-2022-0351`
`cve: CVE-2022-0359`
`cve: CVE-2022-0361`
`cve: CVE-2022-0368`
`cve: CVE-2022-0408`
`cve: CVE-2022-0443`
`cve: CVE-2022-0554`
`cve: CVE-2022-0572`
`cve: CVE-2022-0629`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-0685
cve: CVE-2022-0714
cve: CVE-2022-0729
cve: CVE-2022-2207
advisory_id: USN-6026-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0778
cert-bund: WID-SEC-2022-0509
cert-bund: WID-SEC-2022-0354
cert-bund: WID-SEC-2022-0248
cert-bund: WID-SEC-2022-0151
cert-bund: WID-SEC-2022-0111
cert-bund: WID-SEC-2022-0109
cert-bund: WID-SEC-2022-0108
cert-bund: WID-SEC-2022-0107
cert-bund: WID-SEC-2022-0106
cert-bund: WID-SEC-2022-0059
cert-bund: WID-SEC-2022-0058
cert-bund: WID-SEC-2022-0057
cert-bund: WID-SEC-2022-0056
cert-bund: WID-SEC-2022-0054
cert-bund: WID-SEC-2022-0052
cert-bund: WID-SEC-2022-0050
cert-bund: WID-SEC-2022-0048
cert-bund: CB-K22/0619
cert-bund: CB-K22/0316
dfn-cert: DFN-CERT-2023-0905
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2675
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-1995
dfn-cert: DFN-CERT-2022-1632
dfn-cert: DFN-CERT-2022-1572
dfn-cert: DFN-CERT-2022-1474
dfn-cert: DFN-CERT-2022-1443
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-1262
dfn-cert: DFN-CERT-2022-1250

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1174
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1118
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-0598
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0572
dfn-cert: DFN-CERT-2022-0503
dfn-cert: DFN-CERT-2022-0291
dfn-cert: DFN-CERT-2022-0248
dfn-cert: DFN-CERT-2022-0178
dfn-cert: DFN-CERT-2022-0016

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6267-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6267-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-116.0.3+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6267-1 fixed vulnerabilities and USN-6267-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4051, CVE-2023-4053, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4058)

... continues on next page ...

... continued from previous page ...

Max Vlasov discovered that Firefox Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2023-4045)
Alexander Guryanov discovered that Firefox did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)
Mark Brand discovered that Firefox did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6267-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6267.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6267-3`
`url: https://launchpad.net/bugs/2032143`
`cve: CVE-2023-4045`
`cve: CVE-2023-4046`
`cve: CVE-2023-4047`
`cve: CVE-2023-4048`
`cve: CVE-2023-4049`
`cve: CVE-2023-4050`
`cve: CVE-2023-4051`
`cve: CVE-2023-4053`
`cve: CVE-2023-4055`
`cve: CVE-2023-4056`
`cve: CVE-2023-4057`
`cve: CVE-2023-4058`
`advisory_id: USN-6267-3`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2202`
`cert-bund: WID-SEC-2023-1934`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-2359`
`dfn-cert: DFN-CERT-2023-2358`
`dfn-cert: DFN-CERT-2023-2190`
`dfn-cert: DFN-CERT-2023-2047`
`dfn-cert: DFN-CERT-2023-2028`
`dfn-cert: DFN-CERT-2023-2004`
`dfn-cert: DFN-CERT-2023-1779`
`dfn-cert: DFN-CERT-2023-1761`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6267-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6267-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-116.0.2+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6267-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4051, CVE-2023-4053, CVE-2023-4055, CVE-2023-4056, CVE-2023-4057, CVE-2023-4058)
Max Vlasov discovered that Firefox Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2023-4045)
Alexander Guryanov discovered that Firefox did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)
Mark Brand discovered that Firefox did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6267-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6267.2
Version used: `2024-02-02T04:09:01Z`

. . . continues on next page . . .

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-6267-2
url: https://launchpad.net/bugs/2030690
cve: CVE-2023-4045
cve: CVE-2023-4046
cve: CVE-2023-4047
cve: CVE-2023-4048
cve: CVE-2023-4049
cve: CVE-2023-4050
cve: CVE-2023-4051
cve: CVE-2023-4053
cve: CVE-2023-4055
cve: CVE-2023-4056
cve: CVE-2023-4057
cve: CVE-2023-4058
advisory_id: USN-6267-2
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2202
cert-bund: WID-SEC-2023-1934
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2359
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2047
dfn-cert: DFN-CERT-2023-2028
dfn-cert: DFN-CERT-2023-2004
dfn-cert: DFN-CERT-2023-1779
dfn-cert: DFN-CERT-2023-1761

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6468-1)

Summary

The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6468-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:    thunderbird
Installed version:     thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:115.4.1+build1-0ubuntu0.20.04.1
```

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

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-5724, CVE-2023-5728, CVE-2023-5730, CVE-2023-5732)
Kelsey Gilbert discovered that Thunderbird did not properly manage certain browser prompts and dialogs due to an insufficient activation-delay. An attacker could potentially exploit this issue to perform clickjacking. (CVE-2023-5721)
Shaheen Fazim discovered that Thunderbird did not properly validate the URLs open by installed WebExtension. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-5725)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6468-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6468.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6468-1`
`cve: CVE-2023-5721`
`cve: CVE-2023-5724`
`cve: CVE-2023-5725`
`cve: CVE-2023-5728`
`cve: CVE-2023-5730`
`cve: CVE-2023-5732`
`advisory_id: USN-6468-1`
`cert-bund: WID-SEC-2023-2743`
`dfn-cert: DFN-CERT-2023-2707`
`dfn-cert: DFN-CERT-2023-2698`
`dfn-cert: DFN-CERT-2023-2673`
`dfn-cert: DFN-CERT-2023-2611`
`dfn-cert: DFN-CERT-2023-2608`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5107-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5107-1 advisory.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-93.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof another origin, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5107-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5107.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5107-1
cve: CVE-2021-32810
cve: CVE-2021-38496
cve: CVE-2021-38497
cve: CVE-2021-38498
cve: CVE-2021-38499
cve: CVE-2021-38500
cve: CVE-2021-38501
advisory_id: USN-5107-1
cert-bund: WID-SEC-2022-0689
cert-bund: CB-K21/1045
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2586
dfn-cert: DFN-CERT-2021-2124
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2075
dfn-cert: DFN-CERT-2021-1684

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6405-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6405-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:115.3.1+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4057, CVE-2023-4577, CVE-2023-4578, CVE-2023-4583, CVE-2023-4585, CVE-2023-5169, CVE-2023-5171, CVE-2023-5176)
Andrew McCreight discovered that Thunderbird did not properly manage during the worker lifecycle. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-3600)
Harveer Singh discovered that Thunderbird did not store push notifications in private browsing mode in encrypted form. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-4580)
Clement Lecigne discovered that Thunderbird did not properly manage memory when handling VP8 media stream. An attacker-controlled VP8 media stream could lead to a heap buffer overflow in the content process, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-5217)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6405-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6405.1
Version used: `2024-02-01T08:21:47Z`

References
```
url: https://ubuntu.com/security/notices/USN-6405-1
cve: CVE-2023-3600
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2023-4057
cve: CVE-2023-4577
cve: CVE-2023-4578
cve: CVE-2023-4580
cve: CVE-2023-4583
cve: CVE-2023-4585
cve: CVE-2023-5169
cve: CVE-2023-5171
cve: CVE-2023-5176
cve: CVE-2023-5217
advisory_id: USN-6405-1
cert-bund: WID-SEC-2023-2599
cert-bund: WID-SEC-2023-2572
cert-bund: WID-SEC-2023-2514
cert-bund: WID-SEC-2023-2498
cert-bund: WID-SEC-2023-2448
cert-bund: WID-SEC-2023-2202
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1934
cert-bund: WID-SEC-2023-1866
cert-bund: WID-SEC-2023-1716
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2484
dfn-cert: DFN-CERT-2023-2435
dfn-cert: DFN-CERT-2023-2433
dfn-cert: DFN-CERT-2023-2397
dfn-cert: DFN-CERT-2023-2395
dfn-cert: DFN-CERT-2023-2384
dfn-cert: DFN-CERT-2023-2377
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2357
dfn-cert: DFN-CERT-2023-2348
dfn-cert: DFN-CERT-2023-2344
dfn-cert: DFN-CERT-2023-2330
dfn-cert: DFN-CERT-2023-2310
dfn-cert: DFN-CERT-2023-2285
dfn-cert: DFN-CERT-2023-2281
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2028
dfn-cert: DFN-CERT-2023-2004
dfn-cert: DFN-CERT-2023-1779
dfn-cert: DFN-CERT-2023-1761
dfn-cert: DFN-CERT-2023-1678
dfn-cert: DFN-CERT-2023-1572
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6333-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6333-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.15.0+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Junsung Lee discovered that Thunderbird did not properly validate the text direction override unicode character in filenames. An attacker could potentially exploits this issue by spoofing file extension while attaching a file in emails. (CVE-2023-3417)
Max Vlasov discovered that Thunderbird Offscreen Canvas did not properly track cross-origin tainting. An attacker could potentially exploit this issue to access image data from another site in violation of same-origin policy. (CVE-2023-4045)
Alexander Guryanov discovered that Thunderbird did not properly update the value of a global variable in WASM JIT analysis in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4046)
Mark Brand discovered that Thunderbird did not properly validate the size of an untrusted input stream. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4050)
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4047, CVE-2023-4048, CVE-2023-4049, CVE-2023-4055, CVE-2023-4056)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6333-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6333.1
Version used: `2024-02-02T04:09:01Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6333-1
cve: CVE-2023-3417
cve: CVE-2023-4045
cve: CVE-2023-4046
cve: CVE-2023-4047
cve: CVE-2023-4048
cve: CVE-2023-4049
cve: CVE-2023-4050
cve: CVE-2023-4055
cve: CVE-2023-4056
advisory_id: USN-6333-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1934
cert-bund: WID-SEC-2023-1866
dfn-cert: DFN-CERT-2023-2359
dfn-cert: DFN-CERT-2023-2047
dfn-cert: DFN-CERT-2023-1779
dfn-cert: DFN-CERT-2023-1761
dfn-cert: DFN-CERT-2023-1701
dfn-cert: DFN-CERT-2023-1678
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6214-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6214-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.13.0+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-34414, CVE-2023-34416, CVE-2023-37201, CVE-2023-37202, CVE-2023-37207, CVE-2023-37211)
P Umar Farooq discovered that Thunderbird did not properly provide warning when opening Diagcab files. If a user were tricked into opening a malicious Diagcab file, an attacker could execute arbitrary code. (CVE-2023-37208)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6214-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6214.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6214-1`
`cve: CVE-2023-34414`
`cve: CVE-2023-34416`
`cve: CVE-2023-37201`
`cve: CVE-2023-37202`
`cve: CVE-2023-37207`
`cve: CVE-2023-37208`
`cve: CVE-2023-37211`
`advisory_id: USN-6214-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1663`
`cert-bund: WID-SEC-2023-1414`
`cert-bund: WID-SEC-2023-1385`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-1611`
`dfn-cert: DFN-CERT-2023-1564`
`dfn-cert: DFN-CERT-2023-1531`
`dfn-cert: DFN-CERT-2023-1530`
`dfn-cert: DFN-CERT-2023-1340`
`dfn-cert: DFN-CERT-2023-1335`
`dfn-cert: DFN-CERT-2023-1305`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5411-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5411-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-100.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass permission prompts, obtain sensitive information, bypass security restrictions, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5411-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5411.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5411-1
cve: CVE-2022-29909
cve: CVE-2022-29911
cve: CVE-2022-29912
cve: CVE-2022-29914
cve: CVE-2022-29915
cve: CVE-2022-29916
cve: CVE-2022-29917
cve: CVE-2022-29918
advisory_id: USN-5411-1
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0538
cert-bund: WID-SEC-2022-0537
cert-bund: CB-K22/0542
cert-bund: CB-K22/0534
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1007
dfn-cert: DFN-CERT-2022-1003
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0978

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5824-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5824-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:102.7.1+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45418, CVE-2022-45420, CVE-2022-45421, CVE-2022-46878, CVE-2022-46880, CVE-2022-46881, CVE-2022-46882, CVE-2023-23605)
Armin Ebert discovered that Thunderbird did not properly manage memory while resolving file symlink. If a user were tricked into opening a specially crafted weblink, an attacker could potentially exploit these to cause a denial of service. (CVE-2022-45412)
Sarah Jamie Lewis discovered that Thunderbird did not properly manage network request while handling HTML emails with certain tags. If a user were tricked into opening a specially HTML email, an attacker could potentially exploit these issue and load remote content regardless of a configuration to block remote content. (CVE-2022-45414)
Erik Kraft, Martin Schwarzl, and Andrew McCreight discovered that Thunderbird incorrectly handled keyboard events. An attacker could possibly use this issue to perform a timing side-channel attack and possibly figure out which keys are being pressed. (CVE-2022-45416)

... continues on next page ...

... continued from previous page ...

It was discovered that Thunderbird was using an out-of-date libusrsctp library. An attacker could possibly use this library to perform a reentrancy issue on Thunderbird. (CVE-2022-46871)
Nika Layzell discovered that Thunderbird was not performing a check on paste received from cross-processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)
Matthias Zoellner discovered that Thunderbird was not keeping the filename ending intact when using the drag-and-drop event. An attacker could possibly use this issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)
Hafiizh discovered that Thunderbird was not properly handling fullscreen notifications when the window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)
Tom Schuster discovered that Thunderbird was not performing a validation check on GTK drag data. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23598)
Vadim discovered that Thunderbird was not properly sanitizing a curl command output when copying a network request from the developer tools panel. An attacker could potentially exploits this to hide and execute arbitrary commands. (CVE-2023-23599)
Luan Herrera discovered that Thunderbird was not stopping navigation when dragging a URL from a cross-origin iframe into the same tab. An ... [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-5824-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5824.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5824-1`
`cve: CVE-2022-45403`
`cve: CVE-2022-45404`
`cve: CVE-2022-45405`
`cve: CVE-2022-45406`
`cve: CVE-2022-45408`
`cve: CVE-2022-45409`
`cve: CVE-2022-45410`
`cve: CVE-2022-45411`
`cve: CVE-2022-45412`
`cve: CVE-2022-45414`
`cve: CVE-2022-45416`
`cve: CVE-2022-45418`
`cve: CVE-2022-45420`
`cve: CVE-2022-45421`
`cve: CVE-2022-46871`
`cve: CVE-2022-46872`
`cve: CVE-2022-46874`
`cve: CVE-2022-46877`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-46878
cve: CVE-2022-46880
cve: CVE-2022-46881
cve: CVE-2022-46882
cve: CVE-2023-0430
cve: CVE-2023-23598
cve: CVE-2023-23599
cve: CVE-2023-23601
cve: CVE-2023-23602
cve: CVE-2023-23603
cve: CVE-2023-23605
advisory_id: USN-5824-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0244
cert-bund: WID-SEC-2023-0107
cert-bund: WID-SEC-2022-2319
cert-bund: WID-SEC-2022-2203
cert-bund: WID-SEC-2022-2055
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0408
dfn-cert: DFN-CERT-2023-0242
dfn-cert: DFN-CERT-2023-0150
dfn-cert: DFN-CERT-2023-0146
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2023-0104
dfn-cert: DFN-CERT-2022-2932
dfn-cert: DFN-CERT-2022-2836
dfn-cert: DFN-CERT-2022-2828
dfn-cert: DFN-CERT-2022-2722
dfn-cert: DFN-CERT-2022-2576
dfn-cert: DFN-CERT-2022-2575

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5504-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5504-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-102.0+build2-0ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass CSP restrictions, bypass sandboxed iframe restrictions, obtain sensitive information, bypass the HTML sanitizer, or execute arbitrary code. (CVE-2022-2200, CVE-2022-34468, CVE-2022-34470, CVE-2022-34473, CVE-2022-34474, CVE-2022-34475, CVE-2022-34476, CVE-2022-34477, CVE-2022-34479, CVE-2022-34480, CVE-2022-34481, CVE-2022-34484, CVE-2022-34485)
It was discovered that Firefox could be made to save an image with an executable extension in the filename when dragging and dropping an image in some circumstances. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to trick the user into executing arbitrary code. (CVE-2022-34482, CVE-2022-34483)
It was discovered that a compromised server could trick Firefox into an addon downgrade in some circumstances. An attacker could potentially exploit this to trick the browser into downgrading an addon to a prior version. (CVE-2022-34471)
It was discovered that an unavailable PAC file caused OCSP requests to be blocked, resulting in incorrect error pages being displayed. (CVE-2022-34472)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5504-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5504.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5504-1`
`cve: CVE-2022-2200`
`cve: CVE-2022-34468`
`cve: CVE-2022-34470`
`cve: CVE-2022-34471`
`cve: CVE-2022-34472`
`cve: CVE-2022-34473`
`cve: CVE-2022-34474`
`cve: CVE-2022-34475`
`cve: CVE-2022-34476`
`cve: CVE-2022-34477`
`cve: CVE-2022-34479`
`cve: CVE-2022-34480`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-34481
cve: CVE-2022-34482
cve: CVE-2022-34483
cve: CVE-2022-34484
cve: CVE-2022-34485
advisory_id: USN-5504-1
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-0505
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1535
dfn-cert: DFN-CERT-2022-1524
dfn-cert: DFN-CERT-2022-1441
dfn-cert: DFN-CERT-2022-1440
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6587-3)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6587-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.15
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.15
```

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

Affected Software/OS
'xorg-server, xwayland' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
USN-6587-1 fixed vulnerabilities in X.Org X Server. The fix was incomplete resulting in a possible regression. This update fixes the problem.
We apologize for the inconvenience.

... continues on next page ...

... continued from previous page ...

Original advisory details:
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs. An attacker could possibly use this issue to cause the X Server to crash, obtain sensitive information, or execute arbitrary code. (CVE-2023-6816)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled reattaching to a different master device. An attacker could use this issue to cause the X Server to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2024-0229)
Olivier Fourdan and Donn Seeley discovered that the X.Org X Server incorrectly labeled GLX PBuffers when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service. (CVE-2024-0408)
Olivier Fourdan discovered that the X.Org X Server incorrectly handled the curser code when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service. (CVE-2024-0409)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the XISendDeviceHierarchyEvent API. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21885)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled devices being disabled. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21886)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6587-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6587.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6587-3`
`url: https://launchpad.net/bugs/2051536`
`cve: CVE-2023-6816`
`cve: CVE-2024-0229`
`cve: CVE-2024-0408`
`cve: CVE-2024-0409`
`cve: CVE-2024-21885`
`cve: CVE-2024-21886`
`advisory_id: USN-6587-3`
`cert-bund: WID-SEC-2024-0127`
`dfn-cert: DFN-CERT-2024-1413`
`dfn-cert: DFN-CERT-2024-1393`
`dfn-cert: DFN-CERT-2024-1274`
`dfn-cert: DFN-CERT-2024-1149`
`dfn-cert: DFN-CERT-2024-1145`
`dfn-cert: DFN-CERT-2024-0212`
`dfn-cert: DFN-CERT-2024-0141`
`dfn-cert: DFN-CERT-2024-0130`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4920-1)

Summary
The remote host is missing an update for the 'zeromq3' package(s) announced via the USN-4920-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libzmq5
Installed version:    libzmq5-4.3.2-2ubuntu1
Fixed version:      >=libzmq5-4.3.2-2ubuntu1.20.04.1~esm2
```

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

Affected Software/OS
'zeromq3' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that ZeroMQ incorrectly handled certain application metadata. A remote attacker could use this issue to cause ZeroMQ to crash, or possibly execute arbitrary code. (CVE-2019-13132)
It was discovered that ZeroMQ mishandled certain network traffic. An unauthenticated attacker could use this vulnerability to cause a denial-of- service and prevent legitimate clients from communicating with ZeroMQ. (CVE-2020-15166)
It was discovered that ZeroMQ did not properly manage memory under certain circumstances. If a user or automated system were tricked into connecting to one or multiple compromised servers, a remote attacker could use this issue to cause a denial of service. (CVE-2021-20234)
It was discovered that ZeroMQ incorrectly handled memory when processing messages with arbitrarily large sizes under certain circumstances. A remote unauthenticated attacker could use this issue to cause a ZeroMQ server to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2021-20235)
It was discovered that ZeroMQ did not properly manage memory under certain circumstances. A remote unauthenticated attacker could use this issue to cause a ZeroMQ server to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2021-20237)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4920-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.4920.1
Version used: `2024-02-02T04:09:01Z`

. . . continues on next page . . .

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-4920-1
cve: CVE-2019-13132
cve: CVE-2020-15166
cve: CVE-2021-20234
cve: CVE-2021-20235
cve: CVE-2021-20237
advisory_id: USN-4920-1
cert-bund: CB-K21/1231
dfn-cert: DFN-CERT-2021-0520
dfn-cert: DFN-CERT-2020-2064
dfn-cert: DFN-CERT-2020-1945
dfn-cert: DFN-CERT-2019-1369

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6402-1)

Summary

The remote host is missing an update for the 'libtommath' package(s) announced via the USN-6402-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: libtommath1
Installed version: libtommath1-1.2.0-3
Fixed version: >=libtommath1-1.2.0-3ubuntu0.1

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'libtommath' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight

It was discovered that LibTomMath incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code and cause a denial of service (DoS).

Vulnerability Detection Method

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

Details: Ubuntu: Security Advisory (USN-6402-1)

OID:1.3.6.1.4.1.25623.1.1.12.2023.6402.1

Version used: 2024-02-02T04:09:01Z

... continues on next page ...

. . . continued from previous page . . .

References
url: https://ubuntu.com/security/notices/USN-6402-1
cve: CVE-2023-36328
advisory_id: USN-6402-1
dfn-cert: DFN-CERT-2023-2044

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5402-1)

Summary
The remote host is missing an update for the 'openssl, openssl1.0' package(s) announced via the USN-5402-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssl1.1
Installed version: libssl1.1-1.1.1f-1ubuntu2.4
Fixed version: >=libssl1.1-1.1.1f-1ubuntu2.13

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

Affected Software/OS
'openssl, openssl1.0' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Elison Niven discovered that OpenSSL incorrectly handled the c_rehash script. A local attacker could possibly use this issue to execute arbitrary commands when c_rehash is run. (CVE-2022-1292)
Raul Metsma discovered that OpenSSL incorrectly verified certain response signing certificates. A remote attacker could possibly use this issue to spoof certain response signing certificates. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-1343)
Tom Colley discovered that OpenSSL used the incorrect MAC key in the RC4-MD5 ciphersuite. In non-default configurations were RC4-MD5 is enabled, a remote attacker could possibly use this issue to modify encrypted communications. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-1434)
Aliaksei Levin discovered that OpenSSL incorrectly handled resources when decoding certificates and keys. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-1473)

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-5402-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5402.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5402-1
cve: CVE-2022-1292
cve: CVE-2022-1343
cve: CVE-2022-1434
cve: CVE-2022-1473
advisory_id: USN-5402-1
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2723
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0755
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0555
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0071
cert-bund: CB-K22/0536
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2309
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1875

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1425
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-0986

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5051-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5051-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssl1.1
Installed version: libssl1.1-1.1.1f-1ubuntu2.4
Fixed version: >=libssl1.1-1.1.1f-1ubuntu2.8

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

Affected Software/OS
'openssl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
John Ouyang discovered that OpenSSL incorrectly handled decrypting SM2 data. A remote attacker could use this issue to cause applications using OpenSSL to crash, resulting in a denial of service, or possibly change application behaviour. (CVE-2021-3711)
Ingo Schwarze discovered that OpenSSL incorrectly handled certain ASN.1 strings. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2021-3712)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5051-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5051.1
Version used: 2024-02-02T04:09:01Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5051-1
cve: CVE-2021-3711
cve: CVE-2021-3712
advisory_id: USN-5051-1
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1821
cert-bund: WID-SEC-2023-1030
cert-bund: WID-SEC-2023-0530
cert-bund: WID-SEC-2022-2000
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1894
cert-bund: WID-SEC-2022-1515
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0473
cert-bund: CB-K22/0469
cert-bund: CB-K22/0224
cert-bund: CB-K22/0077
cert-bund: CB-K22/0072
cert-bund: CB-K22/0062
cert-bund: CB-K22/0045
cert-bund: CB-K22/0011
cert-bund: CB-K21/1268
cert-bund: CB-K21/1179
cert-bund: CB-K21/1087
cert-bund: CB-K21/0907
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-2825
dfn-cert: DFN-CERT-2022-2350
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1386
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0922
dfn-cert: DFN-CERT-2022-0867
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0369
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0120
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2022-0031
dfn-cert: DFN-CERT-2021-2481
dfn-cert: DFN-CERT-2021-2434
dfn-cert: DFN-CERT-2021-2403
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2329
dfn-cert: DFN-CERT-2021-2223
dfn-cert: DFN-CERT-2021-2188
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1996
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1799
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5767-1)

Summary
The remote host is missing an update for the 'python2.7, python3.6, python3.8, python3.10' package(s) announced via the USN-5767-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libpython3.8
Installed version:    libpython3.8-3.8.5-1~20.04.3
Fixed version:      >=libpython3.8-3.8.10-0ubuntu1~20.04.6
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.6
```

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

Affected Software/OS
'python2.7, python3.6, python3.8, python3.10' 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 ...

Nicky Mouha discovered that Python incorrectly handled certain SHA-3 internals. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-37454)
It was discovered that Python incorrectly handled certain IDNA inputs. An attacker could possibly use this issue to expose sensitive information denial of service, or cause a crash. (CVE-2022-45061)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5767-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5767.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5767-1`
`cve: CVE-2022-37454`
`cve: CVE-2022-45061`
`advisory_id: USN-5767-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2679`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1793`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1007`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0255`
`cert-bund: WID-SEC-2023-0138`
`cert-bund: WID-SEC-2022-2043`
`cert-bund: WID-SEC-2022-1816`
`dfn-cert: DFN-CERT-2024-0227`
`dfn-cert: DFN-CERT-2023-3168`
`dfn-cert: DFN-CERT-2023-2783`
`dfn-cert: DFN-CERT-2023-1656`
`dfn-cert: DFN-CERT-2023-1517`
`dfn-cert: DFN-CERT-2023-1423`
`dfn-cert: DFN-CERT-2023-1200`
`dfn-cert: DFN-CERT-2023-1109`
`dfn-cert: DFN-CERT-2023-0886`
`dfn-cert: DFN-CERT-2023-0580`
`dfn-cert: DFN-CERT-2023-0571`
`dfn-cert: DFN-CERT-2023-0552`
`dfn-cert: DFN-CERT-2023-0429`
`dfn-cert: DFN-CERT-2023-0422`
`dfn-cert: DFN-CERT-2023-0120`
`dfn-cert: DFN-CERT-2023-0028`
`dfn-cert: DFN-CERT-2022-2869`
`dfn-cert: DFN-CERT-2022-2793`
`dfn-cert: DFN-CERT-2022-2715`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2698
dfn-cert: DFN-CERT-2022-2658
dfn-cert: DFN-CERT-2022-2639
dfn-cert: DFN-CERT-2022-2638
dfn-cert: DFN-CERT-2022-2598
dfn-cert: DFN-CERT-2022-2583
dfn-cert: DFN-CERT-2022-2535
dfn-cert: DFN-CERT-2022-2523
dfn-cert: DFN-CERT-2022-2420
dfn-cert: DFN-CERT-2022-2380

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpam-modules
Installed version: libpam-modules-1.3.1-5ubuntu4.2
Fixed version: >=libpam-modules-1.3.1-5ubuntu4.6

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

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

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-5825-1)

Summary
The remote host is missing an update for the 'pam' package(s) announced via the USN-5825-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpam-modules
Installed version: libpam-modules-1.3.1-5ubuntu4.2
Fixed version: >=libpam-modules-1.3.1-5ubuntu4.4

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
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-5825-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5825.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5825-1
cve: CVE-2022-28321
advisory_id: USN-5825-1

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5168-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5168-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.49.1-1ubuntu1.5
Fixed version:      >=libnss3-2:3.49.1-1ubuntu1.6
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Tavis Ormandy discovered that NSS incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause NSS to crash, resulting in 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-5168-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5168.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5168-1
cve: CVE-2021-43527
advisory_id: USN-5168-1
cert-bund: WID-SEC-2024-0114
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1775
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1766
cert-bund: WID-SEC-2022-0810
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1246
dfn-cert: DFN-CERT-2024-0126
dfn-cert: DFN-CERT-2022-2309
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-1105
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2021-2642
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2563
dfn-cert: DFN-CERT-2021-2499

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5184-1)

Summary
The remote host is missing an update for the 'libmysofa' package(s) announced via the USN-5184-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libmysofa1
Installed version: libmysofa1-1.0~dfsg0-1
Fixed version: >=libmysofa1-1.0~dfsg0-1ubuntu0.1~esm1

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

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

Vulnerability Insight
It was discovered that libmysofa mishandled certain input. An attacker could use this vulnerability to cause a denial of service (crash).

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5184-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5184.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5184-1
cve: CVE-2021-3756
advisory_id: USN-5184-1
dfn-cert: DFN-CERT-2021-2554

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5787-1)

Summary
The remote host is missing an update for the 'libksba' package(s) announced via the USN-5787-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libksba8
Installed version:    libksba8-1.3.5-2
Fixed version:      >=libksba8-1.3.5-2ubuntu0.20.04.2
```

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

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

Vulnerability Insight
It was discovered that Libksba incorrectly handled parsing CRL signatures. A remote attacker could use this issue to cause Libksba to crash, resulting in 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-5787-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5787.1
Version used: 2024-02-02T04:09:01Z

References
```
url: https://ubuntu.com/security/notices/USN-5787-1
cve: CVE-2022-47629
advisory_id: USN-5787-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0419
cert-bund: WID-SEC-2023-0222
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0486
dfn-cert: DFN-CERT-2023-0423
dfn-cert: DFN-CERT-2023-0418
dfn-cert: DFN-CERT-2023-0353
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2288

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5887-1)

Summary
The remote host is missing an update for the 'clamav' package(s) announced via the USN-5887-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: clamav
Installed version: clamav-0.103.2+dfsg-0ubuntu0.20.04.2
Fixed version: >=clamav-0.103.8+dfsg-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Simon Scannell discovered that ClamAV incorrectly handled parsing HFS+ files. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service, or execute arbitrary code. (CVE-2023-20032)
Simon Scannell discovered that ClamAV incorrectly handled parsing DMG files. A remote attacker could possibly use this issue to expose sensitive information. (CVE-2023-20052)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5887-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5887.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5887-1
cve: CVE-2023-20032
cve: CVE-2023-20052
advisory_id: USN-5887-1
cert-bund: WID-SEC-2023-0404
dfn-cert: DFN-CERT-2023-0384

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5688-1)

Summary
The remote host is missing an update for the 'libksba' package(s) announced via the USN-5688-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libksba8
Installed version:    libksba8-1.3.5-2
Fixed version:      >=libksba8-1.3.5-2ubuntu0.20.04.1
```

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

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

Vulnerability Insight
It was discovered that an integer overflow could be triggered in Libksba when decoding certain data. An attacker could use this issue to cause a denial of service (application crash) 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-5688-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5688.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5688-1
cve: CVE-2022-3515
advisory_id: USN-5688-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2022-1744
dfn-cert: DFN-CERT-2022-2664
dfn-cert: DFN-CERT-2022-2288
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5029-1)

. . . continues on next page . . .

... continued from previous page ...

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-5029-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libgnutls30
Installed version:    libgnutls30-3.6.13-2ubuntu1.3
Fixed version:      >=libgnutls30-3.6.13-2ubuntu1.6
```

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

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

Vulnerability Insight
It was discovered that GnuTLS incorrectly handled sending certain extensions when being used as a client. A remote attacker could use this issue to cause GnuTLS to crash, resulting in 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-5029-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5029.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5029-1
cve: CVE-2021-20231
cve: CVE-2021-20232
advisory_id: USN-5029-1
cert-bund: CB-K21/0273
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2360
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1126
dfn-cert: DFN-CERT-2021-0522
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5528-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'freetype' package(s) announced via the USN-5528-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libfreetype6
Installed version:    libfreetype6-2.10.1-2ubuntu0.1
Fixed version:      >=libfreetype6-2.10.1-2ubuntu0.2
```

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

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

Vulnerability Insight
It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, 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-5528-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5528.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5528-1
cve: CVE-2022-27404
cve: CVE-2022-27405
cve: CVE-2022-27406
cve: CVE-2022-31782
advisory_id: USN-5528-1
cert-bund: WID-SEC-2023-2778
cert-bund: WID-SEC-2023-1783
cert-bund: WID-SEC-2023-1020
cert-bund: WID-SEC-2023-1014
cert-bund: WID-SEC-2023-1012
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-0775
cert-bund: CB-K22/0495
dfn-cert: DFN-CERT-2023-0119
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-1625
dfn-cert: DFN-CERT-2022-1219
dfn-cert: DFN-CERT-2022-0947

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6749-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-6749-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libfreerdp2-2
Installed version: libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version: >=libfreerdp2-2-2.6.1+dfsg1-0ubuntu0.20.04.1

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

Affected Software/OS
'freerdp2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled certain context resets. If a user were tricked into connecting to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-22211)
Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-32039, CVE-2024-32040)
Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could possibly use this issue to cause FreeRDP to crash, resulting in a denial of service. (CVE-2024-32041, CVE-2024-32458, CVE-2024-32460)
Evgeny Legerov discovered that FreeRDP incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause FreeRDP clients and servers to crash, resulting in a denial of service. (CVE-2024-32459)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6749-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2024.6749.1
Version used: 2024-04-25T04:09:16Z

References
url: https://ubuntu.com/security/notices/USN-6749-1
cve: CVE-2024-22211
cve: CVE-2024-32039
cve: CVE-2024-32040
cve: CVE-2024-32041
cve: CVE-2024-32458
cve: CVE-2024-32459
cve: CVE-2024-32460
advisory_id: USN-6749-1
cert-bund: WID-SEC-2024-0905
cert-bund: WID-SEC-2024-0162
dfn-cert: DFN-CERT-2024-1096
dfn-cert: DFN-CERT-2024-1084
dfn-cert: DFN-CERT-2024-0291

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6522-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-6522-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libfreerdp2-2
Installed version: libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version: >=libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.6

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

Affected Software/OS
'freerdp2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled drive redirection. If a user were tricked into connection to a malicious server, a remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2022-41877)

... continues on next page ...

... continued from previous page ...

It was discovered that FreeRDP incorrectly handled certain surface updates. A remote attacker could use this issue to cause FreeRDP to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-39352, CVE-2023-39356)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6522-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6522.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6522-1`
`cve: CVE-2022-41877`
`cve: CVE-2023-39352`
`cve: CVE-2023-39356`
`advisory_id: USN-6522-1`
`cert-bund: WID-SEC-2023-2251`
`cert-bund: WID-SEC-2023-1185`
`dfn-cert: DFN-CERT-2023-3005`
`dfn-cert: DFN-CERT-2023-3001`
`dfn-cert: DFN-CERT-2023-2897`
`dfn-cert: DFN-CERT-2023-2420`
`dfn-cert: DFN-CERT-2023-2045`
`dfn-cert: DFN-CERT-2023-0328`
`dfn-cert: DFN-CERT-2022-2725`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6401-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-6401-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libfreerdp2-2
Installed version:    libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version:      >=libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.5
Vulnerable package:   libwinpr2-2
Installed version:    libwinpr2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version:      >=libwinpr2-2-2.2.0+dfsg1-0ubuntu0.20.04.5
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'freerdp2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that FreeRDP did not properly manage certain inputs. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2023-39350, CVE-2023-39351, CVE-2023-39353, CVE-2023-39354, CVE-2023-40181, CVE-2023-40188, CVE-2023-40589)
It was discovered that FreeRDP did not properly manage certain inputs. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-40186, CVE-2023-40567, CVE-2023-40569)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6401-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6401.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6401-1`
`cve: CVE-2023-39350`
`cve: CVE-2023-39351`
`cve: CVE-2023-39353`
`cve: CVE-2023-39354`
`cve: CVE-2023-40181`
`cve: CVE-2023-40186`
`cve: CVE-2023-40188`
`cve: CVE-2023-40567`
`cve: CVE-2023-40569`
`cve: CVE-2023-40589`
`advisory_id: USN-6401-1`
`cert-bund: WID-SEC-2023-2251`
`dfn-cert: DFN-CERT-2023-3005`
`dfn-cert: DFN-CERT-2023-2420`
`dfn-cert: DFN-CERT-2023-2382`
`dfn-cert: DFN-CERT-2023-2045`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5461-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-5461-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libfreerdp-client2-2
Installed version:    libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version:      >=libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.3
```

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

Affected Software/OS
'freerdp2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled empty password values. A remote attacker could use this issue to bypass server authentication. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-24882)
It was discovered that FreeRDP incorrectly handled server configurations with an invalid SAM file path. A remote attacker could use this issue to bypass server authentication. (CVE-2022-24883)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5461-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5461.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5461-1
cve: CVE-2022-24882
cve: CVE-2022-24883
advisory_id: USN-5461-1
dfn-cert: DFN-CERT-2023-2897
dfn-cert: DFN-CERT-2022-0937
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5320-1)

Summary
The remote host is missing an update for the 'expat' package(s) announced via the USN-5320-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.2.9-1build1
Fixed version:      >=libexpat1-2.2.9-1ubuntu0.4
```

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

Affected Software/OS
'expat' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
USN-5288-1 fixed several vulnerabilities in Expat. For CVE-2022-25236 it caused a regression and an additional patch was required. This update address this regression and several other vulnerabilities.
It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-25313)
It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-25314)
It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-25315)
Original advisory details:
It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-25236)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5320-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5320.1
Version used: `2024-02-28T10:02:42Z`

References

```
url: https://ubuntu.com/security/notices/USN-5320-1
url: https://launchpad.net/bugs/1963903
cve: CVE-2022-25313
cve: CVE-2022-25314
cve: CVE-2022-25315
advisory_id: USN-5320-1
cert-bund: WID-SEC-2023-2639
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1335
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1319
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-0857
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0813
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0457
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0063
cert-bund: CB-K22/0208
dfn-cert: DFN-CERT-2023-1919
dfn-cert: DFN-CERT-2023-0832
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2515
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-1962
dfn-cert: DFN-CERT-2022-1680
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1457
dfn-cert: DFN-CERT-2022-1418
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0669
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0623
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0510
dfn-cert: DFN-CERT-2022-0486
dfn-cert: DFN-CERT-2022-0404

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5288-1)

Summary
The remote host is missing an update for the 'expat' package(s) announced via the USN-5288-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.2.9-1build1
Fixed version:      >=libexpat1-2.2.9-1ubuntu0.2
```

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

Affected Software/OS
'expat' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5288-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5288.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5288-1
cve: CVE-2021-45960
cve: CVE-2021-46143
cve: CVE-2022-22822
cve: CVE-2022-22823
cve: CVE-2022-22824
cve: CVE-2022-22825
cve: CVE-2022-22826
cve: CVE-2022-22827
cve: CVE-2022-23852
cve: CVE-2022-23990
cve: CVE-2022-25235
cve: CVE-2022-25236
advisory_id: USN-5288-1
cert-bund: WID-SEC-2023-2639
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1909
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1319
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-0857
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0813
cert-bund: WID-SEC-2022-0798
cert-bund: WID-SEC-2022-0554
cert-bund: WID-SEC-2022-0499
cert-bund: WID-SEC-2022-0498
cert-bund: WID-SEC-2022-0457
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0246
cert-bund: WID-SEC-2022-0062
cert-bund: CB-K22/0485
cert-bund: CB-K22/0220
cert-bund: CB-K22/0114
cert-bund: CB-K22/0091
cert-bund: CB-K22/0055
dfn-cert: DFN-CERT-2024-0609
dfn-cert: DFN-CERT-2024-0605
dfn-cert: DFN-CERT-2023-1919
dfn-cert: DFN-CERT-2023-0832
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2515
dfn-cert: DFN-CERT-2022-2511
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2218
dfn-cert: DFN-CERT-2022-1962
dfn-cert: DFN-CERT-2022-1680
dfn-cert: DFN-CERT-2022-1457
dfn-cert: DFN-CERT-2022-1418
dfn-cert: DFN-CERT-2022-1242
dfn-cert: DFN-CERT-2022-0931
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759
dfn-cert: DFN-CERT-2022-0732
dfn-cert: DFN-CERT-2022-0669
dfn-cert: DFN-CERT-2022-0632
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0623
dfn-cert: DFN-CERT-2022-0620
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0510
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0486
dfn-cert: DFN-CERT-2022-0450
dfn-cert: DFN-CERT-2022-0412
dfn-cert: DFN-CERT-2022-0404
dfn-cert: DFN-CERT-2022-0233
dfn-cert: DFN-CERT-2022-0221
dfn-cert: DFN-CERT-2022-0101

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5310-1)

Summary
The remote host is missing an update for the 'glibc' package(s) announced via the USN-5310-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libc6
Installed version: libc6-2.31-0ubuntu9.2
Fixed version: >=libc6-2.31-0ubuntu9.7

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

Affected Software/OS
'glibc' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Jan Engelhardt, Tavis Ormandy, and others discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could possibly use this issue to cause the GNU C Library to hang or crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2016-10228, CVE-2019-25013, CVE-2020-27618, CVE-2020-29562, CVE-2021-3326)
Jason Royes and Samuel Dytrych discovered that the GNU C Library incorrectly handled signed comparisons on ARMv7 targets. A remote attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-6096)
It was discovered that the GNU C Library nscd daemon incorrectly handled certain netgroup lookups. An attacker could possibly use this issue to cause the GNU C Library to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-27645)

... continues on next page ...

... continued from previous page ...

It was discovered that the GNU C Library wordexp function incorrectly handled certain patterns. An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly obtain sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-35942)
It was discovered that the GNU C Library realpath function incorrectly handled return values. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 21.10. (CVE-2021-3998)
It was discovered that the GNU C library getcwd function incorrectly handled buffers. 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. (CVE-2021-3999)
It was discovered that the GNU C Library sunrpc module incorrectly handled buffer lengths. An attacker could possibly use this issue to cause the GNU C Library to crash, resulting in a denial of service. (CVE-2022-23218, CVE-2022-23219)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5310-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5310.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5310-1`
`cve: CVE-2016-10228`
`cve: CVE-2019-25013`
`cve: CVE-2020-27618`
`cve: CVE-2020-29562`
`cve: CVE-2020-6096`
`cve: CVE-2021-27645`
`cve: CVE-2021-3326`
`cve: CVE-2021-35942`
`cve: CVE-2021-3998`
`cve: CVE-2021-3999`
`cve: CVE-2022-23218`
`cve: CVE-2022-23219`
`advisory_id: USN-5310-1`
`cert-bund: WID-SEC-2024-1186`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0120`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1752`
`cert-bund: WID-SEC-2022-1750`
`cert-bund: WID-SEC-2022-1747`
`cert-bund: WID-SEC-2022-1220`
`cert-bund: WID-SEC-2022-1206`
`cert-bund: WID-SEC-2022-1172`
`cert-bund: WID-SEC-2022-1171`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1170
cert-bund: WID-SEC-2022-1169
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0624
cert-bund: CB-K22/0097
cert-bund: CB-K22/0061
cert-bund: CB-K22/0054
cert-bund: CB-K21/0720
cert-bund: CB-K21/0716
cert-bund: CB-K21/0709
cert-bund: CB-K21/0237
cert-bund: CB-K21/0138
cert-bund: CB-K21/0132
cert-bund: CB-K20/1206
cert-bund: CB-K20/0739
dfn-cert: DFN-CERT-2024-1195
dfn-cert: DFN-CERT-2023-0113
dfn-cert: DFN-CERT-2022-2792
dfn-cert: DFN-CERT-2022-2386
dfn-cert: DFN-CERT-2022-2287
dfn-cert: DFN-CERT-2022-1878
dfn-cert: DFN-CERT-2022-0649
dfn-cert: DFN-CERT-2022-0594
dfn-cert: DFN-CERT-2022-0470
dfn-cert: DFN-CERT-2022-0177
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2500
dfn-cert: DFN-CERT-2021-2377
dfn-cert: DFN-CERT-2021-2059
dfn-cert: DFN-CERT-2021-1615
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1477
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1112
dfn-cert: DFN-CERT-2021-1074
dfn-cert: DFN-CERT-2021-1037
dfn-cert: DFN-CERT-2021-0441
dfn-cert: DFN-CERT-2021-0439
dfn-cert: DFN-CERT-2021-0233
dfn-cert: DFN-CERT-2021-0115
dfn-cert: DFN-CERT-2020-1567
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6587-1)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6587-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.14
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.14
```

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

Affected Software/OS
'xorg-server, xwayland' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the DeviceFocusEvent and ProcXIQueryPointer APIs. An attacker could possibly use this issue to cause the X Server to crash, obtain sensitive information, or execute arbitrary code. (CVE-2023-6816)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled reattaching to a different master device. An attacker could use this issue to cause the X Server to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2024-0229)
Olivier Fourdan and Donn Seeley discovered that the X.Org X Server incorrectly labeled GLX PBuffers when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service. (CVE-2024-0408)
Olivier Fourdan discovered that the X.Org X Server incorrectly handled the curser code when used with SELinux. An attacker could use this issue to cause the X Server to crash, leading to a denial of service. (CVE-2024-0409)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the XISendDeviceHierarchyEvent API. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21885)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled devices being disabled. An attacker could possibly use this issue to cause the X Server to crash, or execute arbitrary code. (CVE-2024-21886)

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-6587-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6587.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6587-1
cve: CVE-2023-6816
cve: CVE-2024-0229
cve: CVE-2024-0408
cve: CVE-2024-0409
cve: CVE-2024-21885
cve: CVE-2024-21886
advisory_id: USN-6587-1
cert-bund: WID-SEC-2024-0127
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1393
dfn-cert: DFN-CERT-2024-1274
dfn-cert: DFN-CERT-2024-1149
dfn-cert: DFN-CERT-2024-1145
dfn-cert: DFN-CERT-2024-0212
dfn-cert: DFN-CERT-2024-0141
dfn-cert: DFN-CERT-2024-0130

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5472-1)

Summary

The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-5472-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: libavcodec58
Installed version: libavcodec58-7:4.2.4-1ubuntu0.1
Fixed version: >=libavcodec58-7:4.2.7-0ubuntu0.1
Vulnerable package: libavformat58
Installed version: libavformat58-7:4.2.4-1ubuntu0.1
Fixed version: >=libavformat58-7:4.2.7-0ubuntu0.1
Vulnerable package: libavutil56
Installed version: libavutil56-7:4.2.4-1ubuntu0.1
Fixed version: >=libavutil56-7:4.2.7-0ubuntu0.1
Vulnerable package: libpostproc55
Installed version: libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version: >=libpostproc55-7:4.2.7-0ubuntu0.1
Vulnerable package: libswresample3

... continues on next page ...

... continued from previous page ...

```
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1
```

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

Affected Software/OS
'ffmpeg' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that FFmpeg would attempt to divide by zero when using Linear Predictive Coding (LPC) or AAC codecs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2020-20445, CVE-2020-20446, CVE-2020-20453)
It was discovered that FFmpeg incorrectly handled certain input. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-20450)
It was discovered that FFmpeg incorrectly handled file conversion to APNG format. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-21041)
It was discovered that FFmpeg incorrectly handled remuxing RTP-hint tracks. A remote attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-21688)
It was discovered that FFmpeg incorrectly handled certain specially crafted AVI files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-21697)
It was discovered that FFmpeg incorrectly handled writing MOV video tags. An attacker could possibly use this issue to cause a denial of service, obtain sensitive information or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2020-22015)
It was discovered that FFmpeg incorrectly handled writing MOV files. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. This issue affected only Ubuntu 18.04 LTS. (CVE-2020-22016)
It was discovered that FFmpeg incorrectly handled memory when using certain filters. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-22017, CVE-2020-22020, CVE-2020-22022, CVE-2020-22023, CVE-2022-22025, CVE-2020-22026, CVE-2020-22028, CVE-2020-22031, CVE-2020-22032, CVE-2020-22034, CVE-2020-22036, CVE-2020-22042)
It was discovered that FFmpeg incorrectly handled memory when using certain filters. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2020-22019, CVE-2020-22021, CVE-2020-22033)

... continues on next page ...

... continued from previous page ...

It was discovered that FFmpeg incorrectly handled memory when using certain filters. An attacker could possibly use this issue to cause a denial of service or other unspecified impact. This issue only affected Ubuntu 21.10. (CVE-2020-22027, CVE-2020-22029, CVE-2020-22030, CVE-2020-22035)
It was discovered that FFmpeg incorrectly handled certain specially crafted JPEG files. An attacker could possibly use ... [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-5472-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5472.1
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-5472-1`
`cve: CVE-2020-20445`
`cve: CVE-2020-20446`
`cve: CVE-2020-20450`
`cve: CVE-2020-20453`
`cve: CVE-2020-21041`
`cve: CVE-2020-21688`
`cve: CVE-2020-21697`
`cve: CVE-2020-22015`
`cve: CVE-2020-22016`
`cve: CVE-2020-22017`
`cve: CVE-2020-22019`
`cve: CVE-2020-22020`
`cve: CVE-2020-22021`
`cve: CVE-2020-22022`
`cve: CVE-2020-22023`
`cve: CVE-2020-22025`
`cve: CVE-2020-22026`
`cve: CVE-2020-22027`
`cve: CVE-2020-22028`
`cve: CVE-2020-22029`
`cve: CVE-2020-22030`
`cve: CVE-2020-22031`
`cve: CVE-2020-22032`
`cve: CVE-2020-22033`
`cve: CVE-2020-22034`
`cve: CVE-2020-22035`
`cve: CVE-2020-22036`
`cve: CVE-2020-22037`
`cve: CVE-2020-22042`
`cve: CVE-2020-35965`
`cve: CVE-2021-38114`
`cve: CVE-2021-38171`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2021-38291
cve: CVE-2022-1475
advisory_id: USN-5472-1
cert-bund: WID-SEC-2023-0011
cert-bund: WID-SEC-2022-0240
cert-bund: WID-SEC-2022-0218
cert-bund: WID-SEC-2022-0216
cert-bund: WID-SEC-2022-0215
cert-bund: WID-SEC-2022-0211
cert-bund: WID-SEC-2022-0210
cert-bund: WID-SEC-2022-0209
cert-bund: WID-SEC-2022-0208
cert-bund: WID-SEC-2022-0206
cert-bund: CB-K22/0528
cert-bund: CB-K21/1013
cert-bund: CB-K21/0870
cert-bund: CB-K21/0832
cert-bund: CB-K21/0747
cert-bund: CB-K21/0746
cert-bund: CB-K21/0599
cert-bund: CB-K21/0581
cert-bund: CB-K21/0566
cert-bund: CB-K21/0002
dfn-cert: DFN-CERT-2024-1464
dfn-cert: DFN-CERT-2024-1134
dfn-cert: DFN-CERT-2023-0013
dfn-cert: DFN-CERT-2022-1293
dfn-cert: DFN-CERT-2022-1122
dfn-cert: DFN-CERT-2021-2409
dfn-cert: DFN-CERT-2021-2268
dfn-cert: DFN-CERT-2021-2242
dfn-cert: DFN-CERT-2021-2199
dfn-cert: DFN-CERT-2021-2088
dfn-cert: DFN-CERT-2021-1997
dfn-cert: DFN-CERT-2021-1863
dfn-cert: DFN-CERT-2021-1855
dfn-cert: DFN-CERT-2021-1748
dfn-cert: DFN-CERT-2021-1502
dfn-cert: DFN-CERT-2021-0201
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5800-1)

Summary
The remote host is missing an update for the 'heimdal' package(s) announced via the USN-5800-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libasn1-8-heimdal
Installed version:    libasn1-8-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libasn1-8-heimdal-7.7.0+dfsg-1ubuntu1.3
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1.3
Vulnerable package:   libhx509-5-heimdal
Installed version:    libhx509-5-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libhx509-5-heimdal-7.7.0+dfsg-1ubuntu1.3
Vulnerable package:   libkrb5-26-heimdal
Installed version:    libkrb5-26-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libkrb5-26-heimdal-7.7.0+dfsg-1ubuntu1.3
```

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

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

Vulnerability Insight
It was discovered that Heimdal incorrectly handled certain SPNEGO tokens. A remote attacker could possibly use this issue to cause a denial of service. (CVE-2021-44758)
Evgeny Legerov discovered that Heimdal incorrectly handled memory when performing certain DES decryption operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-3437)
Greg Hudson discovered that Kerberos PAC implementation used in Heimdal incorrectly handled certain parsing operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-42898)
It was discovered that Heimdal's KDC did not properly handle certain error conditions. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-44640)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5800-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5800.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5800-1
cve: CVE-2021-44758
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-3437
cve: CVE-2022-42898
cve: CVE-2022-44640
advisory_id: USN-5800-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2057
cert-bund: WID-SEC-2022-1847
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2657
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2022-2579
dfn-cert: DFN-CERT-2022-2374
dfn-cert: DFN-CERT-2022-2364

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6447-1)

Summary
The remote host is missing an update for the 'aom' package(s) announced via the USN-6447-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libaom0
Installed version: libaom0-1.0.0.errata1-3build1
Fixed version: >=libaom0-1.0.0.errata1-3+deb11u1build0.20.04.1

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'aom' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that AOM incorrectly handled certain inputs. 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. (CVE-2020-36130, CVE-2020-36131, CVE-2020-36133, CVE-2020-36135, CVE-2021-30473, CVE-2021-30474, CVE-2021-30475)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6447-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6447.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6447-1`
`cve: CVE-2020-36130`
`cve: CVE-2020-36131`
`cve: CVE-2020-36133`
`cve: CVE-2020-36135`
`cve: CVE-2021-30473`
`cve: CVE-2021-30474`
`cve: CVE-2021-30475`
`advisory_id: USN-6447-1`
`dfn-cert: DFN-CERT-2023-2066`
`dfn-cert: DFN-CERT-2021-2672`
`dfn-cert: DFN-CERT-2021-2140`
`dfn-cert: DFN-CERT-2021-1279`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5495-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5495-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package: curl`
`Installed version: curl-7.68.0-1ubuntu2.5`

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=curl-7.68.0-1ubuntu2.12
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.12
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.12
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Harry Sintonen discovered that curl incorrectly handled certain cookies. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 21.10, and Ubuntu 22.04 LTS. (CVE-2022-32205)
Harry Sintonen discovered that curl incorrectly handled certain HTTP compressions. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-32206)
Harry Sintonen incorrectly handled certain file permissions. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 21.10, and Ubuntu 22.04 LTS. (CVE-2022-32207)
Harry Sintonen discovered that curl incorrectly handled certain FTP-KRB messages. An attacker could possibly use this to perform a machine-in-the-middle attack. (CVE-2022-32208)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5495-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5495.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5495-1
cve: CVE-2022-32205
cve: CVE-2022-32206
cve: CVE-2022-32207
cve: CVE-2022-32208
advisory_id: USN-5495-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1424
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0479
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1306
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1830
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1525
dfn-cert: DFN-CERT-2022-1464
dfn-cert: DFN-CERT-2022-1426
```

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-2.0.7-1ubuntu5
Fixed version:      >=klibc-utils-2.0.7-1ubuntu5.2
Vulnerable package:   libklibc
Installed version:    libklibc-2.0.7-1ubuntu5
Fixed version:      >=libklibc-2.0.7-1ubuntu5.2
```

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.

... continues on next page ...

... continued from previous page ...

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

`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-2024-1232`
`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`

... continues on next page ...

... continued from previous page ...

```
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
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
```

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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-5702-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5702-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.14
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.14
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.14
```

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
Robby Simpson discovered that curl incorrectly handled certain POST operations after PUT operations. This issue could cause applications using curl to send the wrong data, perform incorrect memory operations, or crash. (CVE-2022-32221)
Hiroki Kurosawa discovered that curl incorrectly handled parsing .netrc files. If an attacker were able to provide a specially crafted .netrc file, this issue could cause curl to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-35260)
It was discovered that curl incorrectly handled certain HTTP proxy return codes. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-42915)

... continues on next page ...

... continued from previous page ...

Hiroki Kurosawa discovered that curl incorrectly handled HSTS support when certain hostnames included IDN characters. 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-2022-42916)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5702-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5702.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5702-1`
`cve: CVE-2022-32221`
`cve: CVE-2022-35260`
`cve: CVE-2022-42915`
`cve: CVE-2022-42916`
`advisory_id: USN-5702-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2229`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1728`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-1026`
`cert-bund: WID-SEC-2023-0296`
`cert-bund: WID-SEC-2023-0189`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2023-0126`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-1862`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-1636`
`dfn-cert: DFN-CERT-2023-1230`
`dfn-cert: DFN-CERT-2023-0898`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0372`
`dfn-cert: DFN-CERT-2023-0278`
`dfn-cert: DFN-CERT-2023-0216`
`dfn-cert: DFN-CERT-2023-0214`
`dfn-cert: DFN-CERT-2023-0157`
`dfn-cert: DFN-CERT-2023-0156`
`dfn-cert: DFN-CERT-2023-0105`
`dfn-cert: DFN-CERT-2022-2799`
`dfn-cert: DFN-CERT-2022-2401`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2400
dfn-cert: DFN-CERT-2022-2393
dfn-cert: DFN-CERT-2022-2391

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5379-1)

Summary
The remote host is missing an update for the 'klibc' package(s) announced via the USN-5379-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   klibc-utils
Installed version:    klibc-utils-2.0.7-1ubuntu5
Fixed version:      >=klibc-utils-2.0.7-1ubuntu5.1
Vulnerable package:   libklibc
Installed version:    libklibc-2.0.7-1ubuntu5
Fixed version:      >=libklibc-2.0.7-1ubuntu5.1
```

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.

Vulnerability Insight
It was discovered that klibc did not properly perform some mathematical operations, leading to an integer overflow. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31870)
It was discovered that klibc did not properly handled some memory allocations on 64 bit systems. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31871)
It was discovered that klibc did not properly handled some file sizes values on 32 bit systems. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31872)
It was discovered that klibc did not properly handled some memory allocations. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-31873)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5379-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2022.5379.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5379-1
cve: CVE-2021-31870
cve: CVE-2021-31871
cve: CVE-2021-31872
cve: CVE-2021-31873
advisory_id: USN-5379-1
dfn-cert: DFN-CERT-2021-1394

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6783-1)

Summary
The remote host is missing an update for the 'vlc' package(s) announced via the USN-6783-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vlc-plugin-base
Installed version: vlc-plugin-base-3.0.9.2-1
Fixed version: >=vlc-plugin-base-3.0.9.2-1ubuntu0.1~esm2

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

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

Vulnerability Insight
It was discovered that VLC incorrectly handled certain media files. A remote attacker could possibly use this issue to cause VLC to crash, resulting in a denial of service, or potential arbitrary code execution.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6783-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6783.1
Version used: 2024-05-24T04:08:05Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6783-1
cve: CVE-2023-47359
cve: CVE-2023-47360
advisory_id: USN-6783-1
cert-bund: WID-SEC-2023-2857
dfn-cert: DFN-CERT-2023-3018
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6429-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-6429-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.20
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.20
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.20
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Jay Satiro discovered that curl incorrectly handled hostnames when using a SOCKS5 proxy. In environments where curl is configured to use a SOCKS5 proxy, a remote attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-38545)
It was discovered that curl incorrectly handled cookies when an application duplicated certain handles. A local attacker could possibly create a cookie file and inject arbitrary cookies into subsequent connections. (CVE-2023-38546)

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-6429-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6429.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6429-1
cve: CVE-2023-38545
cve: CVE-2023-38546
advisory_id: USN-6429-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0893
cert-bund: WID-SEC-2024-0290
cert-bund: WID-SEC-2024-0178
cert-bund: WID-SEC-2024-0175
cert-bund: WID-SEC-2024-0123
cert-bund: WID-SEC-2024-0119
cert-bund: WID-SEC-2024-0110
cert-bund: WID-SEC-2023-2788
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2570
dfn-cert: DFN-CERT-2024-1090
dfn-cert: DFN-CERT-2024-1025
dfn-cert: DFN-CERT-2024-0963
dfn-cert: DFN-CERT-2024-0869
dfn-cert: DFN-CERT-2024-0376
dfn-cert: DFN-CERT-2024-0185
dfn-cert: DFN-CERT-2024-0184
dfn-cert: DFN-CERT-2024-0181
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2024-0132
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3064
dfn-cert: DFN-CERT-2023-2988
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2763
dfn-cert: DFN-CERT-2023-2680
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2475
dfn-cert: DFN-CERT-2023-2458

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5810-2)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5810-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   git
Installed version:    git-1:2.25.1-1ubuntu3.1
Fixed version:      >=git-1:2.25.1-1ubuntu3.8
```

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

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

Vulnerability Insight
USN-5810-1 fixed vulnerabilities in Git. This update introduced a regression as it was missing some commit lines. This update fixes the problem.
Original advisory details:
Markus Vervier and Eric Sesterhenn discovered that Git incorrectly handled certain gitattributes. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-23521)
Joern Schneeweisz discovered that Git incorrectly handled certain commands. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-41903)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5810-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5810.2
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5810-2
url: https://launchpad.net/bugs/2003246
cve: CVE-2022-23521
cve: CVE-2022-41903
advisory_id: USN-5810-2
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0105
dfn-cert: DFN-CERT-2023-0884
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0843
dfn-cert: DFN-CERT-2023-0274
dfn-cert: DFN-CERT-2023-0108

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5810-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5810-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.25.1-1ubuntu3.1
Fixed version: >=git-1:2.25.1-1ubuntu3.7

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

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

Vulnerability Insight
Markus Vervier and Eric Sesterhenn discovered that Git incorrectly handled certain gitattributes. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-23521)
Joern Schneeweisz discovered that Git incorrectly handled certain commands. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-41903)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5810-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5810.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5810-1
cve: CVE-2022-23521
cve: CVE-2022-41903
advisory_id: USN-5810-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1424

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0105
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0843
dfn-cert: DFN-CERT-2023-0274
dfn-cert: DFN-CERT-2023-0108

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6017-1)

Summary
The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-6017-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   ghostscript
Installed version:    ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version:      >=ghostscript-9.50~dfsg-5ubuntu4.7
Vulnerable package:   libgs9
Installed version:    libgs9-9.50~dfsg-5ubuntu4.2
Fixed version:      >=libgs9-9.50~dfsg-5ubuntu4.7
```

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

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

Vulnerability Insight
Hadrien Perrineau discovered that Ghostscript incorrectly handled certain inputs. 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-6017-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6017.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6017-1
cve: CVE-2023-28879
advisory_id: USN-6017-1
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-0827
dfn-cert: DFN-CERT-2023-2877
dfn-cert: DFN-CERT-2023-2767
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-0754

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6456-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6456-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-119.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6456-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5722, CVE-2023-5724, CVE-2023-5728, CVE-2023-5729, CVE-2023-5730, CVE-2023-5731)
Kelsey Gilbert discovered that Firefox did not properly manage certain browser prompts and dialogs due to an insufficient activation-delay. An attacker could potentially exploit this issue to perform clickjacking. (CVE-2023-5721)
Daniel Veditz discovered that Firefox did not properly validate a cookie containing invalid characters. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5723)

... continues on next page ...

... continued from previous page ...

Shaheen Fazim discovered that Firefox did not properly validate the URLs open by installed WebExtension. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-5725)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6456-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6456.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6456-2`
`url: https://launchpad.net/bugs/2043441`
`cve: CVE-2023-5721`
`cve: CVE-2023-5722`
`cve: CVE-2023-5723`
`cve: CVE-2023-5724`
`cve: CVE-2023-5725`
`cve: CVE-2023-5728`
`cve: CVE-2023-5729`
`cve: CVE-2023-5730`
`cve: CVE-2023-5731`
`advisory_id: USN-6456-2`
`cert-bund: WID-SEC-2023-2743`
`dfn-cert: DFN-CERT-2023-2707`
`dfn-cert: DFN-CERT-2023-2698`
`dfn-cert: DFN-CERT-2023-2673`
`dfn-cert: DFN-CERT-2023-2611`
`dfn-cert: DFN-CERT-2023-2608`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6456-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6456-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-119.0+build2-0ubuntu0.20.04.1
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5722, CVE-2023-5724, CVE-2023-5728, CVE-2023-5729, CVE-2023-5730, CVE-2023-5731)
Kelsey Gilbert discovered that Firefox did not properly manage certain browser prompts and dialogs due to an insufficient activation-delay. An attacker could potentially exploit this issue to perform clickjacking. (CVE-2023-5721)
Daniel Veditz discovered that Firefox did not properly validate a cookie containing invalid characters. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5723)
Shaheen Fazim discovered that Firefox did not properly validate the URLs open by installed WebExtension. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-5725)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6456-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6456.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6456-1`
`cve: CVE-2023-5721`
`cve: CVE-2023-5722`
`cve: CVE-2023-5723`
`cve: CVE-2023-5724`
`cve: CVE-2023-5725`
`cve: CVE-2023-5728`
`cve: CVE-2023-5729`
`cve: CVE-2023-5730`
`cve: CVE-2023-5731`
`advisory_id: USN-6456-1`
`cert-bund: WID-SEC-2023-2743`
`dfn-cert: DFN-CERT-2023-2707`
`dfn-cert: DFN-CERT-2023-2698`
`dfn-cert: DFN-CERT-2023-2673`
`dfn-cert: DFN-CERT-2023-2611`
`dfn-cert: DFN-CERT-2023-2608`

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-6404-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6404-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-118.0.2+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6404-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-5169, CVE-2023-5170, CVE-2023-5171, CVE-2023-5172, CVE-2023-5175, CVE-2023-5176)
Ronald Crane discovered that Firefox did not properly manage memory when non-HTTPS Alternate Services (network.http.altsvc.oe) is enabled. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-5173)
Clement Lecigne discovered that Firefox did not properly manage memory when handling VP8 media stream. An attacker-controlled VP8 media stream could lead to a heap buffer overflow in the content process, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-5217)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6404-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6404.2
Version used: `2024-02-01T08:21:47Z`

References
```
url: https://ubuntu.com/security/notices/USN-6404-2
url: https://launchpad.net/bugs/2038977
```

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2023-5169
cve: CVE-2023-5170
cve: CVE-2023-5171
cve: CVE-2023-5172
cve: CVE-2023-5173
cve: CVE-2023-5175
cve: CVE-2023-5176
cve: CVE-2023-5217
advisory_id: USN-6404-2
cert-bund: WID-SEC-2023-2599
cert-bund: WID-SEC-2023-2572
cert-bund: WID-SEC-2023-2514
cert-bund: WID-SEC-2023-2498
cert-bund: WID-SEC-2023-2448
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2484
dfn-cert: DFN-CERT-2023-2435
dfn-cert: DFN-CERT-2023-2433
dfn-cert: DFN-CERT-2023-2397
dfn-cert: DFN-CERT-2023-2395
dfn-cert: DFN-CERT-2023-2384
dfn-cert: DFN-CERT-2023-2377
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2357
dfn-cert: DFN-CERT-2023-2348
dfn-cert: DFN-CERT-2023-2344
dfn-cert: DFN-CERT-2023-2330
dfn-cert: DFN-CERT-2023-2310
dfn-cert: DFN-CERT-2023-2285
dfn-cert: DFN-CERT-2023-2281

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5321-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5321-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

Fixed version: >=firefox-98.0.2+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
USN-5321-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information, or execute arbitrary code. (CVE-2022-0843, CVE-2022-26381, CVE-2022-26382, CVE-2022-26383, CVE-2022-26384, CVE-2022-26385)
A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature. (CVE-2022-26387)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5321-3)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5321.3
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5321-3
url: https://launchpad.net/bugs/1966306
cve: CVE-2022-0843
cve: CVE-2022-26381
cve: CVE-2022-26382
cve: CVE-2022-26383
cve: CVE-2022-26384
cve: CVE-2022-26385
cve: CVE-2022-26387
advisory_id: USN-5321-3
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1034
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0283
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0688
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0551
dfn-cert: DFN-CERT-2022-0516

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5321-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5321-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-98.0+build3-0ubuntu0.20.04.2

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information, or execute arbitrary code. (CVE-2022-0843, CVE-2022-26381, CVE-2022-26382, CVE-2022-26383, CVE-2022-26384, CVE-2022-26385)
A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature. (CVE-2022-26387)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5321-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5321.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5321-1
cve: CVE-2022-0843
cve: CVE-2022-26381
cve: CVE-2022-26382
cve: CVE-2022-26383
cve: CVE-2022-26384
cve: CVE-2022-26385
cve: CVE-2022-26387
advisory_id: USN-5321-1
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1034
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0283
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0688
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0551
dfn-cert: DFN-CERT-2022-0516

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5314-1)

Summary

The remote host is missing an update for the 'firefox' package(s) announced via the USN-5314-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-97.0.2+build1-0ubuntu0.20.04.1

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
A use-after-free was discovered when removing an XSLT parameter in some circumstances. If a user were tricked into opening a specially crafted website, an attacker could exploit this to cause a denial of service, or execute arbitrary code. (CVE-2022-26485)
A use-after-free was discovered in the WebGPU IPC framework. If a user were tricked into opening a specially crafted website, an attacker could exploit this to cause a denial of service, or execute arbitrary code. (CVE-2022-26486)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5314-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5314.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5314-1`
`cve: CVE-2022-26485`
`cve: CVE-2022-26486`
`advisory_id: USN-5314-1`
`cert-bund: WID-SEC-2023-0838`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-1032`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K22/0269`
`dfn-cert: DFN-CERT-2022-0583`
`dfn-cert: DFN-CERT-2022-0559`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0505`

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5345-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5345-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  thunderbird`

... continues on next page ...

... continued from previous page ...

```
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:91.7.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, obtain sensitive information, cause undefined behaviour, spoof the browser UI, or execute arbitrary code. (CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22763, CVE-2022-22764, CVE-2022-26381, CVE-2022-26383, CVE-2022-26384)
It was discovered that extensions of a particular type could auto-update themselves and bypass the prompt that requests permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to bypass security restrictions. (CVE-2022-22754)
It was discovered that dragging and dropping an image into a folder could result in it being marked as executable. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to execute arbitrary code. (CVE-2022-22756)
It was discovered that files downloaded to /tmp were accessible to other users. A local attacker could exploit this to obtain sensitive information. (CVE-2022-26386)
A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature. (CVE-2022-26387)
An out-of-bounds write by one byte was discovered when processing messages in some circumstances. If a user were tricked into opening a specially crafted message, an attacker could potentially exploit this to cause a denial of service. (CVE-2022-0566)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5345-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5345.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5345-1`
`cve: CVE-2022-0566`
`cve: CVE-2022-22754`
`cve: CVE-2022-22756`
`cve: CVE-2022-22759`
`cve: CVE-2022-22760`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-22761
cve: CVE-2022-22763
cve: CVE-2022-22764
cve: CVE-2022-26381
cve: CVE-2022-26383
cve: CVE-2022-26384
cve: CVE-2022-26386
cve: CVE-2022-26387
advisory_id: USN-5345-1
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1034
cert-bund: WID-SEC-2022-1031
cert-bund: WID-SEC-2022-0690
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0283
cert-bund: CB-K22/0195
cert-bund: CB-K22/0157
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0688
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0551
dfn-cert: DFN-CERT-2022-0516
dfn-cert: DFN-CERT-2022-0362
dfn-cert: DFN-CERT-2022-0352
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0296

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5284-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5284-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-97.0+build2-0ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, obtain sensitive information, or execute arbitrary code. (CVE-2022-0511, CVE-2022-22755, CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22764)
It was discovered that extensions of a particular type could auto-update themselves and bypass the prompt that requests permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to bypass security restrictions. (CVE-2022-22754)
It was discovered that dragging and dropping an image into a folder could result in it being marked as executable. If a user were tricked into dragging and dropping a specially crafted image, an attacker could potentially exploit this to execute arbitrary code. (CVE-2022-22756)
It was discovered that Remote Agent, used in WebDriver, did not validate Host or Origin headers. If a user were tricked into opening a specially crafted website with WebDriver enabled, an attacker could potentially exploit this to connect back to the user's browser in order to control it. (CVE-2022-22757)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5284-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5284.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5284-1`
`cve: CVE-2022-0511`
`cve: CVE-2022-22754`
`cve: CVE-2022-22755`
`cve: CVE-2022-22756`
`cve: CVE-2022-22757`
`cve: CVE-2022-22759`
`cve: CVE-2022-22760`
`cve: CVE-2022-22761`
`cve: CVE-2022-22764`
`advisory_id: USN-5284-1`
`cert-bund: WID-SEC-2023-0838`
`cert-bund: WID-SEC-2022-0690`
`cert-bund: WID-SEC-2022-0432`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0157
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0352
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0296

High (CVSS: 9.6)
NVT: Ubuntu: Security Advisory (USN-5321-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5321-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-98.0.1+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
USN-5321-1 fixed vulnerabilities in Firefox. The update didn't include arm64 because of a regression. This update provides the corresponding update for arm64.
This update also removes Yandex and Mail.ru as optional search providers in the drop-down search menu.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information, or execute arbitrary code. (CVE-2022-0843, CVE-2022-26381, CVE-2022-26382, CVE-2022-26383, CVE-2022-26384, CVE-2022-26385)
A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature. (CVE-2022-26387)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5321-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5321.2
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5321-2
cve: CVE-2022-0843
cve: CVE-2022-26381
cve: CVE-2022-26382
cve: CVE-2022-26383
cve: CVE-2022-26384
cve: CVE-2022-26385
cve: CVE-2022-26387
advisory_id: USN-5321-2
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1034
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0283
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0688
dfn-cert: DFN-CERT-2022-0675
dfn-cert: DFN-CERT-2022-0583
dfn-cert: DFN-CERT-2022-0559
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0551
dfn-cert: DFN-CERT-2022-0516

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5155-1)

Summary

The remote host is missing an update for the 'bluez' package(s) announced via the USN-5155-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: bluez
Installed version: bluez-5.53-0ubuntu3.2
Fixed version: >=bluez-5.53-0ubuntu3.4
Vulnerable package: libbluetooth3
Installed version: libbluetooth3-5.53-0ubuntu3.2

... continues on next page ...

... continued from previous page ...

Fixed version: >=libbluetooth3-5.53-0ubuntu3.4

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

Affected Software/OS
'bluez' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that BlueZ incorrectly handled the Discoverable status when a device is powered down. This could result in devices being powered up discoverable, contrary to expectations. This issue only affected Ubuntu 20.04 LTS, Ubuntu 21.04, and Ubuntu 21.10. (CVE-2021-3658)
It was discovered that BlueZ incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause BlueZ to consume resources, leading to a denial of service. (CVE-2021-41229)
It was discovered that the BlueZ gatt server incorrectly handled disconnects. A remote attacker could possibly use this issue to cause BlueZ to crash, leading to a denial of service. (CVE-2021-43400)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5155-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5155.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5155-1
cve: CVE-2021-3658
cve: CVE-2021-41229
cve: CVE-2021-43400
advisory_id: USN-5155-1
cert-bund: WID-SEC-2022-1836
cert-bund: CB-K22/0573
dfn-cert: DFN-CERT-2024-0166
dfn-cert: DFN-CERT-2022-2578
dfn-cert: DFN-CERT-2022-2362
dfn-cert: DFN-CERT-2022-2356
dfn-cert: DFN-CERT-2022-1050
dfn-cert: DFN-CERT-2021-2478
dfn-cert: DFN-CERT-2021-2464
dfn-cert: DFN-CERT-2021-1619

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5099-1)

Summary
The remote host is missing an update for the 'imlib2' package(s) announced via the USN-5099-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libimlib2
Installed version:    libimlib2-1.6.1-1
Fixed version:      >=libimlib2-1.6.1-1ubuntu0.1
```

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

Affected Software/OS
'imlib2' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that Imlib2 incorrectly handled certain ICO images. An attacker could use this issue to cause a denial of service and possibly execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5099-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5099.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5099-1
cve: CVE-2020-12761
advisory_id: USN-5099-1
dfn-cert: DFN-CERT-2021-2055
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5079-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5079-1 advisory.

Quality of Detection: 97

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.7
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.7
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.7
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that curl incorrect handled memory when sending data to an MQTT server. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-22945)
Patrick Monnerat discovered that curl incorrectly handled upgrades to TLS. When receiving certain responses from servers, curl would continue without TLS even when the option to require a successful upgrade to TLS was specified. (CVE-2021-22946)
Patrick Monnerat discovered that curl incorrectly handled responses received before STARTTLS. A remote attacker could possibly use this issue to inject responses and intercept communications. (CVE-2021-22947)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5079-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5079.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5079-1
cve: CVE-2021-22945
cve: CVE-2021-22946
cve: CVE-2021-22947
advisory_id: USN-5079-1
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0875
cert-bund: WID-SEC-2022-0751
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: CB-K22/0316
cert-bund: CB-K22/0077
cert-bund: CB-K22/0062
cert-bund: CB-K22/0030
cert-bund: CB-K21/0991
cert-bund: CB-K21/0969
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0052
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-1931
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5627-1)

Summary
The remote host is missing an update for the 'pcre2' package(s) announced via the USN-5627-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libpcre2-16-0
Installed version:    libpcre2-16-0-10.34-7
Fixed version:      >=libpcre2-16-0-10.34-7ubuntu0.1
Vulnerable package:   libpcre2-32-0
Installed version:    libpcre2-32-0-10.34-7
Fixed version:      >=libpcre2-32-0-10.34-7ubuntu0.1
Vulnerable package:   libpcre2-8-0
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    libpcre2-8-0-10.34-7
Fixed version:      >=libpcre2-8-0-10.34-7ubuntu0.1
Vulnerable package:   libpcre2-posix2
Installed version:    libpcre2-posix2-10.34-7
Fixed version:      >=libpcre2-posix2-10.34-7ubuntu0.1
```

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

Affected Software/OS
'pcre2' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that PCRE incorrectly handled memory when handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to expose sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5627-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5627.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5627-1
cve: CVE-2022-1586
cve: CVE-2022-1587
advisory_id: USN-5627-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1763
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-0523
cert-bund: CB-K22/0602
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0581
dfn-cert: DFN-CERT-2022-2314
dfn-cert: DFN-CERT-2022-1726
dfn-cert: DFN-CERT-2022-1666
dfn-cert: DFN-CERT-2022-1192
dfn-cert: DFN-CERT-2022-1084
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-5777-1)

Summary
The remote host is missing an update for the 'pillow' package(s) announced via the USN-5777-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-pil
Installed version:    python3-pil-7.0.0-4ubuntu0.4
Fixed version:      >=python3-pil-7.0.0-4ubuntu0.7
```

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

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

Vulnerability Insight
It was discovered that Pillow incorrectly handled the deletion of temporary files when using a temporary directory that contains spaces. An attacker could possibly use this issue to delete arbitrary files. This issue only affected Ubuntu 20.04 LTS. (CVE-2022-24303)
It was discovered that Pillow incorrectly handled the decompression of highly compressed GIF data. An attacker could possibly use this issue to cause Pillow to crash, resulting in a denial of service. (CVE-2022-45198)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5777-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5777.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5777-1
cve: CVE-2022-24303
cve: CVE-2022-45198
advisory_id: USN-5777-1
dfn-cert: DFN-CERT-2022-2849
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-0697
```

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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.16
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.16
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.16
```

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 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: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5891-1`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2023-23914
cve: CVE-2023-23915
cve: CVE-2023-23916
advisory_id: USN-5891-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2676
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2101
cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0405
dfn-cert: DFN-CERT-2024-0963
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1636
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1306
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1141
dfn-cert: DFN-CERT-2023-0727
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0385
dfn-cert: DFN-CERT-2023-0371

High (CVSS: 9.0)
NVT: Ubuntu: Security Advisory (USN-5839-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5839-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: apache2
Installed version: apache2-2.4.41-4ubuntu3.3
Fixed version: >=apache2-2.4.41-4ubuntu3.13

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'apache2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that the Apache HTTP Server mod_dav module incorrectly handled certain If: request headers. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2006-20001)
ZeddYu_Lu discovered that the Apache HTTP Server mod_proxy_ajp module incorrectly interpreted certain HTTP Requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. (CVE-2022-36760)
Dimas Fariski Setyawan Putra discovered that the Apache HTTP Server mod_proxy module incorrectly truncated certain response headers. This may result in later headers not being interpreted by the client. (CVE-2022-37436)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5839-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5839.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5839-1`
`cve: CVE-2006-20001`
`cve: CVE-2022-36760`
`cve: CVE-2022-37436`
`advisory_id: USN-5839-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2674`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1022`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0110`
`dfn-cert: DFN-CERT-2023-2545`
`dfn-cert: DFN-CERT-2023-1895`
`dfn-cert: DFN-CERT-2023-1297`
`dfn-cert: DFN-CERT-2023-0658`
`dfn-cert: DFN-CERT-2023-0548`
`dfn-cert: DFN-CERT-2023-0497`
`dfn-cert: DFN-CERT-2023-0118`

High (CVSS: 9.0)
NVT: Ubuntu: Security Advisory (USN-6793-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-6793-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   git
Installed version:    git-1:2.25.1-1ubuntu3.1
Fixed version:      >=git-1:2.25.1-1ubuntu3.12
```

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

Affected Software/OS
'git' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
It was discovered that Git incorrectly handled certain submodules. An attacker could possibly use this issue to execute arbitrary code. This issue was fixed in Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2024-32002)
It was discovered that Git incorrectly handled certain cloned repositories. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-32004)
It was discovered that Git incorrectly handled local clones with hardlinked files/directories. An attacker could possibly use this issue to place a specialized repository on their target's local system. (CVE-2024-32020)
It was discovered that Git incorrectly handled certain symlinks. An attacker could possibly use this issue to impact availability and integrity creating hardlinked arbitrary files into users repository's objects/directory. (CVE-2024-32021)
It was discovered that Git incorrectly handled certain cloned repositories. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-32465)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6793-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6793.1
Version used: `2024-05-29T04:09:43Z`

References
```
url: https://ubuntu.com/security/notices/USN-6793-1
cve: CVE-2024-32002
cve: CVE-2024-32004
cve: CVE-2024-32020
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2024-32021
cve: CVE-2024-32465
advisory_id: USN-6793-1
cert-bund: WID-SEC-2024-1125
cert-bund: WID-SEC-2024-1115
dfn-cert: DFN-CERT-2024-1296
dfn-cert: DFN-CERT-2024-1292

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5292-2)

Summary
The remote host is missing an update for the 'snapd' package(s) announced via the USN-5292-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: snapd
Installed version: snapd-2.49.2+20.04
Fixed version: >=snapd-2.54.3+20.04.1

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

Affected Software/OS
'snapd' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-5292-1 fixed vulnerabilities in snapd. This update provides the corresponding update for the riscv64 architecture.
Original advisory details:
James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. (CVE-2021-3155)
Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. (CVE-2021-4120)
The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. (CVE-2021-44730)
The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code. (CVE-2021-44731)

... 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-5292-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5292.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5292-2`
`cve: CVE-2021-3155`
`cve: CVE-2021-4120`
`cve: CVE-2021-44730`
`cve: CVE-2021-44731`
`advisory_id: USN-5292-2`
`cert-bund: CB-K22/0212`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0406`
`dfn-cert: DFN-CERT-2022-0387`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6544-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-6544-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   binutils
Installed version:    binutils-2.34-6ubuntu1.1
Fixed version:      >=binutils-2.34-6ubuntu1.7
```

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

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

Vulnerability Insight
It was discovered that GNU binutils incorrectly handled certain COFF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS. (CVE-2022-38533)

... continues on next page ...

... continued from previous page ...

It was discovered that GNU binutils was not properly performing bounds checks in several functions, which could lead to a buffer overflow. An attacker could possibly use this issue to cause a denial of service, expose sensitive information or execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-4285, CVE-2020-19726, CVE-2021-46174)
It was discovered that GNU binutils contained a reachable assertion, which could lead to an intentional assertion failure when processing certain crafted DWARF files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-35205)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6544-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6544.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6544-1`
`cve: CVE-2020-19726`
`cve: CVE-2021-46174`
`cve: CVE-2022-35205`
`cve: CVE-2022-38533`
`cve: CVE-2022-4285`
`advisory_id: USN-6544-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2165`
`cert-bund: WID-SEC-2022-2228`
`cert-bund: WID-SEC-2022-1192`
`dfn-cert: DFN-CERT-2023-3082`
`dfn-cert: DFN-CERT-2023-2386`
`dfn-cert: DFN-CERT-2023-2222`
`dfn-cert: DFN-CERT-2023-2183`
`dfn-cert: DFN-CERT-2023-1194`
`dfn-cert: DFN-CERT-2022-2861`
`dfn-cert: DFN-CERT-2022-2757`
`dfn-cert: DFN-CERT-2022-2655`
`dfn-cert: DFN-CERT-2022-2427`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5275-1)

Summary
The remote host is missing an update for the 'bluez' package(s) announced via the USN-5275-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   bluez
Installed version:    bluez-5.53-0ubuntu3.2
Fixed version:      >=bluez-5.53-0ubuntu3.5
Vulnerable package:   libbluetooth3
Installed version:    libbluetooth3-5.53-0ubuntu3.2
Fixed version:      >=libbluetooth3-5.53-0ubuntu3.5
```

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

Affected Software/OS
'bluez' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Ziming Zhang discovered that BlueZ incorrectly handled memory write operations in its gatt server. A remote attacker could possibly use this to cause BlueZ to crash leading to a denial of service, or potentially remotely execute code. (CVE-2022-0204)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5275-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5275.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5275-1
cve: CVE-2022-0204
advisory_id: USN-5275-1
dfn-cert: DFN-CERT-2022-2362
dfn-cert: DFN-CERT-2022-1915
dfn-cert: DFN-CERT-2022-0295
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6083-1)

Summary
The remote host is missing an update for the 'cups-filters' package(s) announced via the USN-6083-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   cups-filters
Installed version:    cups-filters-1.27.4-1
Fixed version:      >=cups-filters-1.27.4-1ubuntu0.2
```

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

Affected Software/OS
'cups-filters' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that cups-filters incorrectly handled the beh CUPS backend. A remote attacker could possibly use this issue to cause the backend to stop responding or to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6083-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6083.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6083-1
cve: CVE-2023-24805
advisory_id: USN-6083-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1245
dfn-cert: DFN-CERT-2023-2542
dfn-cert: DFN-CERT-2023-1202
dfn-cert: DFN-CERT-2023-1149
```

High (CVSS: 8.8)
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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.18
```

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.18
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.18
```

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: `2024-02-02T04:09:01Z`

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-2024-0794
cert-bund: WID-SEC-2023-2694
cert-bund: WID-SEC-2023-2229
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0690
dfn-cert: DFN-CERT-2024-0713
dfn-cert: DFN-CERT-2024-0230
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2776
dfn-cert: DFN-CERT-2023-1939
dfn-cert: DFN-CERT-2023-1827
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1448
dfn-cert: DFN-CERT-2023-1285
dfn-cert: DFN-CERT-2023-1196
dfn-cert: DFN-CERT-2023-1141
dfn-cert: DFN-CERT-2023-1056
dfn-cert: DFN-CERT-2023-0935
dfn-cert: DFN-CERT-2023-0727
dfn-cert: DFN-CERT-2023-0617

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5011-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5011-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-90.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, overlay text over another domain, or 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-5011-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5011.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5011-1
cve: CVE-2021-29970
cve: CVE-2021-29972
cve: CVE-2021-29974
cve: CVE-2021-29975
cve: CVE-2021-29976
cve: CVE-2021-29977
cve: CVE-2021-30547
advisory_id: USN-5011-1
cert-bund: WID-SEC-2022-1112
cert-bund: CB-K21/0753
cert-bund: CB-K21/0645
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1492
dfn-cert: DFN-CERT-2021-1481
dfn-cert: DFN-CERT-2021-1479
dfn-cert: DFN-CERT-2021-1259

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5037-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5037-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-91.0+build2-0ubuntu0.20.04.1

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

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5037-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5037.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5037-1`
`cve: CVE-2021-29980`
`cve: CVE-2021-29981`
`cve: CVE-2021-29982`
`cve: CVE-2021-29984`
`cve: CVE-2021-29985`
`cve: CVE-2021-29986`
`cve: CVE-2021-29987`
`cve: CVE-2021-29988`
`cve: CVE-2021-29989`
`cve: CVE-2021-29990`
`advisory_id: USN-5037-1`
`cert-bund: WID-SEC-2022-1022`
`cert-bund: CB-K21/0861`
`dfn-cert: DFN-CERT-2021-1871`
`dfn-cert: DFN-CERT-2021-1732`
`dfn-cert: DFN-CERT-2021-1728`
`dfn-cert: DFN-CERT-2021-1700`
`dfn-cert: DFN-CERT-2021-1695`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5074-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5074-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-92.0+build3-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass mixed content blocking, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5074-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5074.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5074-1`
`cve: CVE-2021-38491`
`cve: CVE-2021-38493`
`cve: CVE-2021-38494`
`advisory_id: USN-5074-1`
`cert-bund: WID-SEC-2022-1024`
`cert-bund: CB-K21/0939`
`dfn-cert: DFN-CERT-2021-2095`
`dfn-cert: DFN-CERT-2021-1889`
`dfn-cert: DFN-CERT-2021-1888`
`dfn-cert: DFN-CERT-2021-1871`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5186-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5186-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-95.0+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct spoofing attacks, bypass CSP restrictions, or execute arbitrary code. (CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43546)
A security issue was discovered with the handling of WebExtension permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to create and install a service worker that wouldn't be uninstalled with the extension. (CVE-2021-43540)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5186-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5186.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5186-1
cve: CVE-2021-43536
cve: CVE-2021-43537
cve: CVE-2021-43538
cve: CVE-2021-43539
cve: CVE-2021-43540
cve: CVE-2021-43541
cve: CVE-2021-43542
cve: CVE-2021-43543
cve: CVE-2021-43545
cve: CVE-2021-43546
advisory_id: USN-5186-1
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2022-1029
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1255
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0110
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2642
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2549
dfn-cert: DFN-CERT-2021-2548

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5186-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5186-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-95.0.1+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
USN-5186-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct spoofing attacks, bypass CSP restrictions, or execute arbitrary code. (CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43546)
A security issue was discovered with the handling of WebExtension permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to create and install a service worker that wouldn't be uninstalled with the extension. (CVE-2021-43540)

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-5186-2)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5186.2
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5186-2
url: https://launchpad.net/bugs/1955433
cve: CVE-2021-43536
cve: CVE-2021-43537
cve: CVE-2021-43538
cve: CVE-2021-43539
cve: CVE-2021-43540
cve: CVE-2021-43541
cve: CVE-2021-43542
cve: CVE-2021-43543
cve: CVE-2021-43545
cve: CVE-2021-43546
advisory_id: USN-5186-2
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2022-1029
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1255
dfn-cert: DFN-CERT-2022-0110
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2642
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2549
dfn-cert: DFN-CERT-2021-2548

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5370-1)

Summary

The remote host is missing an update for the 'firefox' package(s) announced via the USN-5370-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-99.0+build2-0ubuntu0.20.04.2

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, execute script unexpectedly, obtain sensitive information, conduct spoofing attacks, or execute arbitrary code. (CVE-2022-1097, CVE-2022-24713, CVE-2022-28281, CVE-2022-28282, CVE-2022-28284, CVE-2022-28285, CVE-2022-28286, CVE-2022-28288, CVE-2022-28289)
A security issue was discovered with the sourceMapURL feature of devtools. An attacker could potentially exploit this to include local files that should have been inaccessible. (CVE-2022-28283)
It was discovered that selecting text caused Firefox to crash in some circumstances. An attacker could potentially exploit this to cause a denial of service. (CVE-2022-28287)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5370-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5370.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5370-1`
`cve: CVE-2022-1097`
`cve: CVE-2022-24713`
`cve: CVE-2022-28281`
`cve: CVE-2022-28282`
`cve: CVE-2022-28283`
`cve: CVE-2022-28284`
`cve: CVE-2022-28285`
`cve: CVE-2022-28286`
`cve: CVE-2022-28287`
`cve: CVE-2022-28288`
`cve: CVE-2022-28289`
`advisory_id: USN-5370-1`
`cert-bund: WID-SEC-2023-0838`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0482`
`cert-bund: CB-K22/0396`
`dfn-cert: DFN-CERT-2023-2061`
`dfn-cert: DFN-CERT-2023-0847`
`dfn-cert: DFN-CERT-2022-2557`
`dfn-cert: DFN-CERT-2022-1430`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0769
dfn-cert: DFN-CERT-2022-0763
dfn-cert: DFN-CERT-2022-0762
dfn-cert: DFN-CERT-2022-0553

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5434-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5434-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-100.0.2+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that the methods of an Array object could be corrupted as a result of prototype pollution by sending a message to the parent process. If a user were tricked into opening a specially crafted website, an attacker could exploit this to execute JavaScript in a privileged context.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5434-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5434.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5434-1
cve: CVE-2022-1529
cve: CVE-2022-1802
advisory_id: USN-5434-1
cert-bund: WID-SEC-2022-1251

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0129
cert-bund: CB-K22/0642
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
dfn-cert: DFN-CERT-2022-1162

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5581-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5581-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-104.0+build3-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the contents of the addressbar, bypass security restrictions, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5581-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5581.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5581-1
cve: CVE-2022-38472
cve: CVE-2022-38473
cve: CVE-2022-38475
cve: CVE-2022-38477

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-38478
advisory_id: USN-5581-1
cert-bund: WID-SEC-2022-1167
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2225
dfn-cert: DFN-CERT-2022-2179
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1865
dfn-cert: DFN-CERT-2022-1864

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5649-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5649-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-105.0+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass Content Security Policy (CSP) or other security restrictions, conduct session fixation attacks, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5649-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5649.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5649-1

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-3266
cve: CVE-2022-40956
cve: CVE-2022-40957
cve: CVE-2022-40958
cve: CVE-2022-40959
cve: CVE-2022-40960
cve: CVE-2022-40962
advisory_id: USN-5649-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1497
cert-bund: WID-SEC-2022-1484
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2551
dfn-cert: DFN-CERT-2022-2104
dfn-cert: DFN-CERT-2022-2090
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5709-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5709-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-106.0.2+build1-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42930, CVE-2022-42932)
It was discovered that Firefox saved usernames to a plaintext file. A local user could potentially exploit this to obtain sensitive information. (CVE-2022-42931)

... 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-5709-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5709.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5709-1`
`cve: CVE-2022-42927`
`cve: CVE-2022-42928`
`cve: CVE-2022-42929`
`cve: CVE-2022-42930`
`cve: CVE-2022-42931`
`cve: CVE-2022-42932`
`advisory_id: USN-5709-1`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-1791`
`dfn-cert: DFN-CERT-2022-2551`
`dfn-cert: DFN-CERT-2022-2369`
`dfn-cert: DFN-CERT-2022-2301`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5709-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5709-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-106.0.5+build1-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
USN-5709-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

... continues on next page ...

... continued from previous page ...

We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42930, CVE-2022-42932)
It was discovered that Firefox saved usernames to a plaintext file. A local user could potentially exploit this to obtain sensitive information. (CVE-2022-42931)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5709-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5709.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5709-2`
`url: https://launchpad.net/bugs/1996178`
`cve: CVE-2022-42927`
`cve: CVE-2022-42928`
`cve: CVE-2022-42929`
`cve: CVE-2022-42930`
`cve: CVE-2022-42931`
`cve: CVE-2022-42932`
`advisory_id: USN-5709-2`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-1791`
`dfn-cert: DFN-CERT-2022-2551`
`dfn-cert: DFN-CERT-2022-2369`
`dfn-cert: DFN-CERT-2022-2301`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5782-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5782-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-108.0+build2-0ubuntu0.20.04.1
```

Solution:

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
It was discovered that Firefox was using an out-of-date libusrsctp library. An attacker could possibly use this library to perform a reentrancy issue on Firefox. (CVE-2022-46871)
Nika Layzell discovered that Firefox was not performing a check on paste received from cross-processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)
Pete Freitag discovered that Firefox did not implement the unsafe-hashes CSP directive. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2022-46873)
Matthias Zoellner discovered that Firefox was not keeping the filename ending intact when using the drag-and-drop event. An attacker could possibly use this issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)
Hafiizh discovered that Firefox was not handling fullscreen notifications when the browser window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-46878, CVE-2022-46879)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5782-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5782.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5782-1`
`cve: CVE-2022-46871`
`cve: CVE-2022-46872`
`cve: CVE-2022-46873`
`cve: CVE-2022-46874`
`cve: CVE-2022-46877`
`cve: CVE-2022-46878`
`cve: CVE-2022-46879`
`advisory_id: USN-5782-1`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2319`
`dfn-cert: DFN-CERT-2023-0408`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0150
dfn-cert: DFN-CERT-2023-0146
dfn-cert: DFN-CERT-2023-0104
dfn-cert: DFN-CERT-2022-2932
dfn-cert: DFN-CERT-2022-2836
dfn-cert: DFN-CERT-2022-2828

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5782-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5782-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-108.0.1+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
USN-5782-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Firefox was using an out-of-date libusrsctp library. An attacker could possibly use this library to perform a reentrancy issue on Firefox. (CVE-2022-46871)
Nika Layzell discovered that Firefox was not performing a check on paste received from cross-processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)
Pete Freitag discovered that Firefox did not implement the unsafe-hashes CSP directive. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2022-46873)
Matthias Zoellner discovered that Firefox was not keeping the filename ending intact when using the drag-and-drop event. An attacker could possibly use this issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)

... continues on next page ...

... continued from previous page ...

Hafiizh discovered that Firefox was not handling fullscreen notifications when the browser window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-46878, CVE-2022-46879)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5782-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5782.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5782-2`
`url: https://launchpad.net/bugs/2001921`
`cve: CVE-2022-46871`
`cve: CVE-2022-46872`
`cve: CVE-2022-46873`
`cve: CVE-2022-46874`
`cve: CVE-2022-46877`
`cve: CVE-2022-46878`
`cve: CVE-2022-46879`
`advisory_id: USN-5782-2`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-2319`
`dfn-cert: DFN-CERT-2023-0408`
`dfn-cert: DFN-CERT-2023-0150`
`dfn-cert: DFN-CERT-2023-0146`
`dfn-cert: DFN-CERT-2023-0104`
`dfn-cert: DFN-CERT-2022-2932`
`dfn-cert: DFN-CERT-2022-2836`
`dfn-cert: DFN-CERT-2022-2828`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5782-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5782-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-108.0.2+build1-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
USN-5782-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Firefox was using an out-of-date libusrsctp library. An attacker could possibly use this library to perform a reentrancy issue on Firefox. (CVE-2022-46871)
Nika Layzell discovered that Firefox was not performing a check on paste received from cross-processes. An attacker could potentially exploit this to obtain sensitive information. (CVE-2022-46872)
Pete Freitag discovered that Firefox did not implement the unsafe-hashes CSP directive. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2022-46873)
Matthias Zoellner discovered that Firefox was not keeping the filename ending intact when using the drag-and-drop event. An attacker could possibly use this issue to add a file with a malicious extension, leading to execute arbitrary code. (CVE-2022-46874)
Hafiizh discovered that Firefox was not handling fullscreen notifications when the browser window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2022-46877)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2022-46878, CVE-2022-46879)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5782-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5782.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5782-3`
`url: https://launchpad.net/bugs/2002377`
`cve: CVE-2022-46871`
`cve: CVE-2022-46872`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-46873
cve: CVE-2022-46874
cve: CVE-2022-46877
cve: CVE-2022-46878
cve: CVE-2022-46879
advisory_id: USN-5782-3
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-2319
dfn-cert: DFN-CERT-2023-0408
dfn-cert: DFN-CERT-2023-0150
dfn-cert: DFN-CERT-2023-0146
dfn-cert: DFN-CERT-2023-0104
dfn-cert: DFN-CERT-2022-2932
dfn-cert: DFN-CERT-2022-2836
dfn-cert: DFN-CERT-2022-2828
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5816-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5816-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-109.0+build2-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
Niklas Baumstark discovered that a compromised web child process of Firefox could disable web security opening restrictions, leading to a new child process being spawned within the file:// context. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23597)
Tom Schuster discovered that Firefox was not performing a validation check on GTK drag data. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23598)

... continues on next page ...

... continued from previous page ...

Vadim discovered that Firefox was not properly sanitizing a curl command output when copying a network request from the developer tools panel. An attacker could potentially exploits this to hide and execute arbitrary commands. (CVE-2023-23599)
Luan Herrera discovered that Firefox was not stopping navigation when dragging a URL from a cross-origin iframe into the same tab. An attacker potentially exploits this to spoof the user. (CVE-2023-23601)
Dave Vandyke discovered that Firefox did not properly implement CSP policy when creating a WebSocket in a WebWorker. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2023-23602)
Dan Veditz discovered that Firefox did not properly implement CSP policy on regular expression when using console.log. An attacker potentially exploits this to exfiltrate data from the browser. (CVE-2023-23603)
Nika Layzell discovered that Firefox was not performing a validation check when parsing a non-system html document via DOMParser::ParseFromSafeString. An attacker potentially exploits this to bypass web security checks. (CVE-2023-23604)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-23605, CVE-2023-23606)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5816-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5816.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5816-1`
`cve: CVE-2023-23597`
`cve: CVE-2023-23598`
`cve: CVE-2023-23599`
`cve: CVE-2023-23601`
`cve: CVE-2023-23602`
`cve: CVE-2023-23603`
`cve: CVE-2023-23604`
`cve: CVE-2023-23605`
`cve: CVE-2023-23606`
`advisory_id: USN-5816-1`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0107`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0408`
`dfn-cert: DFN-CERT-2023-0146`
`dfn-cert: DFN-CERT-2023-0104`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5816-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5816-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-109.0.1+build1-0ubuntu0.20.04.2
```

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

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

Vulnerability Insight
USN-5816-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Niklas Baumstark discovered that a compromised web child process of Firefox could disable web security opening restrictions, leading to a new child process being spawned within the file:// context. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23597)
Tom Schuster discovered that Firefox was not performing a validation check on GTK drag data. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-23598)
Vadim discovered that Firefox was not properly sanitizing a curl command output when copying a network request from the developer tools panel. An attacker could potentially exploits this to hide and execute arbitrary commands. (CVE-2023-23599)
Luan Herrera discovered that Firefox was not stopping navigation when dragging a URL from a cross-origin iframe into the same tab. An attacker potentially exploits this to spoof the user. (CVE-2023-23601)
Dave Vandyke discovered that Firefox did not properly implement CSP policy when creating a WebSocket in a WebWorker. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject an executable script. (CVE-2023-23602)
Dan Veditz discovered that Firefox did not properly implement CSP policy on regular expression when using console.log. An attacker potentially exploits this to exfiltrate data from the browser. (CVE-2023-23603)

... continues on next page ...

... continued from previous page ...

Nika Layzell discovered that Firefox was not performing a validation check when parsing a non-system html document via DOMParser::ParseFromSafeString. An attacker potentially exploits this to bypass web security checks. (CVE-2023-23604)
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-23605, CVE-2023-23606)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5816-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5816.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5816-2`
`url: https://launchpad.net/bugs/2006075`
`cve: CVE-2023-23597`
`cve: CVE-2023-23598`
`cve: CVE-2023-23599`
`cve: CVE-2023-23601`
`cve: CVE-2023-23602`
`cve: CVE-2023-23603`
`cve: CVE-2023-23604`
`cve: CVE-2023-23605`
`cve: CVE-2023-23606`
`advisory_id: USN-5816-2`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0107`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0408`
`dfn-cert: DFN-CERT-2023-0146`
`dfn-cert: DFN-CERT-2023-0104`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5954-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5954-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  firefox`
`Installed version:  firefox-89.0.1+build1-0ubuntu0.20.04.1`

... continues on next page ...

... continued from previous page ...

Fixed version: >=firefox-111.0+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25750, CVE-2023-25752, CVE-2023-28162, CVE-2023-28176, CVE-2023-28177)
Lukas Bernhard discovered that Firefox did not properly manage memory when invalidating JIT code while following an iterator. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25751)
Rob Wu discovered that Firefox did not properly manage the URLs when following a redirect to a publicly accessible web extension file. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-28160)
Luan Herrera discovered that Firefox did not properly manage cross-origin iframe when dragging a URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-28164)
Khiem Tran discovered that Firefox did not properly manage one-time permissions granted to a document loaded using a file: URL. An attacker could potentially exploit this issue to use granted one-time permissions on the local files came from different sources. (CVE-2023-28161)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5954-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5954.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5954-1
cve: CVE-2023-25750
cve: CVE-2023-25751
cve: CVE-2023-25752
cve: CVE-2023-28160
cve: CVE-2023-28161
cve: CVE-2023-28162
cve: CVE-2023-28164
cve: CVE-2023-28176
cve: CVE-2023-28177
advisory_id: USN-5954-1
cert-bund: WID-SEC-2023-1424

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0673
cert-bund: WID-SEC-2023-0643
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0741
dfn-cert: DFN-CERT-2023-0738
dfn-cert: DFN-CERT-2023-0579
dfn-cert: DFN-CERT-2023-0557

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5954-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5954-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-111.0.1+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
USN-5954-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-25750, CVE-2023-25752, CVE-2023-28162, CVE-2023-28176, CVE-2023-28177)
Lukas Bernhard discovered that Firefox did not properly manage memory when invalidating JIT code while following an iterator. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25751)
Rob Wu discovered that Firefox did not properly manage the URLs when following a redirect to a publicly accessible web extension file. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-28160)

... continues on next page ...

... continued from previous page ...

Luan Herrera discovered that Firefox did not properly manage cross-origin iframe when dragging a URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-28164)
Khiem Tran discovered that Firefox did not properly manage one-time permissions granted to a document loaded using a file: URL. An attacker could potentially exploit this issue to use granted one-time permissions on the local files came from different sources. (CVE-2023-28161)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5954-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5954.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5954-2`
`url: https://launchpad.net/bugs/2012696`
`cve: CVE-2023-25750`
`cve: CVE-2023-25751`
`cve: CVE-2023-25752`
`cve: CVE-2023-28160`
`cve: CVE-2023-28161`
`cve: CVE-2023-28162`
`cve: CVE-2023-28164`
`cve: CVE-2023-28176`
`cve: CVE-2023-28177`
`advisory_id: USN-5954-2`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0673`
`cert-bund: WID-SEC-2023-0643`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0741`
`dfn-cert: DFN-CERT-2023-0738`
`dfn-cert: DFN-CERT-2023-0579`
`dfn-cert: DFN-CERT-2023-0557`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6010-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6010-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-112.0+build2-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-29537, CVE-2023-29540, CVE-2023-29543, CVE-2023-29544, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551)
Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)
Lukas Bernhard discovered that Firefox did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29535)
Zx from qriousec discovered that Firefox did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29536)
Alexis aka zoracon discovered that Firefox did not properly validate the URI received by the WebExtension during a load request. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-29538)
Trung Pham discovered that Firefox did not properly validate the filename directive in the Content-Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)
Ameen Basha M K discovered that Firefox did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6010-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6010.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6010-1`
`cve: CVE-2023-29533`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2023-29535
cve: CVE-2023-29536
cve: CVE-2023-29537
cve: CVE-2023-29538
cve: CVE-2023-29539
cve: CVE-2023-29540
cve: CVE-2023-29541
cve: CVE-2023-29543
cve: CVE-2023-29544
cve: CVE-2023-29547
cve: CVE-2023-29548
cve: CVE-2023-29549
cve: CVE-2023-29550
cve: CVE-2023-29551
advisory_id: USN-6010-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0941
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0937
dfn-cert: DFN-CERT-2023-0805
dfn-cert: DFN-CERT-2023-0804
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6010-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6010-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-112.0.1+build1-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

USN-6010-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-29537, CVE-2023-29540, CVE-2023-29543, CVE-2023-29544, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551)
Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)
Lukas Bernhard discovered that Firefox did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29535)
Zx from qriousec discovered that Firefox did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29536)
Alexis aka zoracon discovered that Firefox did not properly validate the URI received by the WebExtension during a load request. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-29538)
Trung Pham discovered that Firefox did not properly validate the filename directive in the Content-Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)
Ameen Basha M K discovered that Firefox did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6010-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6010.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6010-2`
`url: https://launchpad.net/bugs/2016835`
`cve: CVE-2023-29533`
`cve: CVE-2023-29535`
`cve: CVE-2023-29536`
`cve: CVE-2023-29537`
`cve: CVE-2023-29538`
`cve: CVE-2023-29539`
`cve: CVE-2023-29540`
`cve: CVE-2023-29541`
`cve: CVE-2023-29543`

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-29544
cve: CVE-2023-29547
cve: CVE-2023-29548
cve: CVE-2023-29549
cve: CVE-2023-29550
cve: CVE-2023-29551
advisory_id: USN-6010-2
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0941
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0937
dfn-cert: DFN-CERT-2023-0805
dfn-cert: DFN-CERT-2023-0804

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6010-3)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6010-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-112.0.2+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
USN-6010-1 fixed vulnerabilities and USN-6010-2 fixed minor regressions in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-29537, CVE-2023-29540, CVE-2023-29543, CVE-2023-29544, CVE-2023-29547, CVE-2023-29548, CVE-2023-29549, CVE-2023-29550, CVE-2023-29551)

... continues on next page ...

... continued from previous page ...

Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)
Lukas Bernhard discovered that Firefox did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29535)
Zx from qriousec discovered that Firefox did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29536)
Alexis aka zoracon discovered that Firefox did not properly validate the URI received by the WebExtension during a load request. An attacker could potentially exploits this to obtain sensitive information. (CVE-2023-29538)
Trung Pham discovered that Firefox did not properly validate the filename directive in the Content-Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)
Ameen Basha M K discovered that Firefox did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6010-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6010.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6010-3`
`url: https://launchpad.net/bugs/2017722`
`cve: CVE-2023-29533`
`cve: CVE-2023-29535`
`cve: CVE-2023-29536`
`cve: CVE-2023-29537`
`cve: CVE-2023-29538`
`cve: CVE-2023-29539`
`cve: CVE-2023-29540`
`cve: CVE-2023-29541`
`cve: CVE-2023-29543`
`cve: CVE-2023-29544`
`cve: CVE-2023-29547`
`cve: CVE-2023-29548`
`cve: CVE-2023-29549`
`cve: CVE-2023-29550`
`cve: CVE-2023-29551`
`advisory_id: USN-6010-3`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-0941`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0937
dfn-cert: DFN-CERT-2023-0805
dfn-cert: DFN-CERT-2023-0804

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6201-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6201-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-115.0+build2-0ubuntu0.20.04.3

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-37201, CVE-2023-37202, CVE-2023-37205, CVE-2023-37207, CVE-2023-37209, CVE-2023-37210, CVE-2023-37211, CVE-2023-37212)
Martin Hostettler discovered that Firefox did not properly block storage of all cookies when configured. An attacker could potentially exploits this issue to store tracking data without permission in localstorage. (CVE-2023-3482)
Paul Nickerson discovered that Firefox did have insufficient validation in the Drag and Drop API. If a user were tricked into creating a shortcut to local system files, an attacker could execute arbitrary code. (CVE-2023-37203)
Irvan Kurniawan discovered that Firefox did not properly manage fullscreen notifications using an option element having an expensive computational function. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-37204)
Ameen Basha M K discovered that Firefox did not properly validate symlinks in the FileSystem API. If a user were tricked into uploading a symlinked file to a malicious website, an attacker could obtain sensitive information. (CVE-2023-37206)

... continues on next page ...

... continued from previous page ...

Puf discovered that Firefox did not properly provide warning when opening Diagcab files. If a user were tricked into opening a malicious Diagcab file, an attacker could execute arbitrary code. (CVE-2023-37208)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6201-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6201.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6201-1`
`cve: CVE-2023-3482`
`cve: CVE-2023-37201`
`cve: CVE-2023-37202`
`cve: CVE-2023-37203`
`cve: CVE-2023-37204`
`cve: CVE-2023-37205`
`cve: CVE-2023-37206`
`cve: CVE-2023-37207`
`cve: CVE-2023-37208`
`cve: CVE-2023-37209`
`cve: CVE-2023-37210`
`cve: CVE-2023-37211`
`cve: CVE-2023-37212`
`advisory_id: USN-6201-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1663`
`dfn-cert: DFN-CERT-2023-1611`
`dfn-cert: DFN-CERT-2023-1564`
`dfn-cert: DFN-CERT-2023-1531`
`dfn-cert: DFN-CERT-2023-1530`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6218-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6218-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  firefox`
`Installed version:  firefox-89.0.1+build1-0ubuntu0.20.04.1`

... continues on next page ...

... continued from previous page ...

Fixed version: >=firefox-115.0.2+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
A use-after-free was discovered in Firefox when handling workers. An attacker could potentially exploit this to cause a denial of service, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6218-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6218.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6218-1
cve: CVE-2023-3600
advisory_id: USN-6218-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1866
cert-bund: WID-SEC-2023-1716
dfn-cert: DFN-CERT-2023-2397
dfn-cert: DFN-CERT-2023-2395
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-1678
dfn-cert: DFN-CERT-2023-1572

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6320-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6320-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-117.0+build2-0ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4578, CVE-2023-4581, CVE-2023-4583, CVE-2023-4584, CVE-2023-4585)
Lukas Bernhard discovered that Firefox did not properly manage memory when the 'UpdateRegExpStatics' attempted to access 'initialStringHeap'. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-4577)
Malte Jurgens discovered that Firefox did not properly handle search queries if the search query itself was a well formed URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-4579)
Harveer Singh discovered that Firefox did not properly handle push notifications stored on disk in private browsing mode. An attacker could potentially exploits this issue to access sensitive information. (CVE-2023-4580)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6320-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6320.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6320-1`
`cve: CVE-2023-4573`
`cve: CVE-2023-4574`
`cve: CVE-2023-4575`
`cve: CVE-2023-4577`
`cve: CVE-2023-4578`
`cve: CVE-2023-4579`
`cve: CVE-2023-4580`
`cve: CVE-2023-4581`
`cve: CVE-2023-4583`
`cve: CVE-2023-4584`
`cve: CVE-2023-4585`
`advisory_id: USN-6320-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2202`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2542
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2152
dfn-cert: DFN-CERT-2023-2028
dfn-cert: DFN-CERT-2023-2004

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6367-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6367-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-117.0.1+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that Firefox did not properly manage memory when handling WebP images. If a user were tricked into opening a webpage containing malicious WebP image file, an attacker could potentially exploit these to cause a denial of service or execute arbitrary code. (CVE-2023-4863)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6367-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6367.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6367-1
cve: CVE-2023-4863
advisory_id: USN-6367-1

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-3099
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2841
cert-bund: WID-SEC-2023-2548
cert-bund: WID-SEC-2023-2538
cert-bund: WID-SEC-2023-2313
cert-bund: WID-SEC-2023-2310
cert-bund: WID-SEC-2023-2305
dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2356
dfn-cert: DFN-CERT-2023-2325
dfn-cert: DFN-CERT-2023-2303
dfn-cert: DFN-CERT-2023-2283
dfn-cert: DFN-CERT-2023-2282
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2176
dfn-cert: DFN-CERT-2023-2152
dfn-cert: DFN-CERT-2023-2149
dfn-cert: DFN-CERT-2023-2120
dfn-cert: DFN-CERT-2023-2119
dfn-cert: DFN-CERT-2023-2110
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6509-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6509-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-120.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-6206, CVE-2023-6210, CVE-2023-6211, CVE-2023-6212, CVE-2023-6213)

It was discovered that Firefox did not properly manage memory when images were created on the canvas element. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6204)

It discovered that Firefox incorrectly handled certain memory when using a MessagePort. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6205)

It discovered that Firefox incorrectly did not properly manage ownership in ReadableByteStreams. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6207)

It discovered that Firefox incorrectly did not properly manage copy operations when using Selection API in X11. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6208)

Rachmat Abdul Rokhim discovered that Firefox incorrectly handled parsing of relative URLS starting with '///'. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6209)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6509-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6509.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-6509-1`
`cve: CVE-2023-6204`
`cve: CVE-2023-6205`
`cve: CVE-2023-6206`
`cve: CVE-2023-6207`
`cve: CVE-2023-6208`
`cve: CVE-2023-6209`
`cve: CVE-2023-6210`
`cve: CVE-2023-6211`
`cve: CVE-2023-6212`
`cve: CVE-2023-6213`
`advisory_id: USN-6509-1`
`cert-bund: WID-SEC-2023-2995`
`dfn-cert: DFN-CERT-2024-0174`
`dfn-cert: DFN-CERT-2023-3078`
`dfn-cert: DFN-CERT-2023-2922`
`dfn-cert: DFN-CERT-2023-2920`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6509-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6509-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-120.0.1+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6509-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2023-6206, CVE-2023-6210, CVE-2023-6211, CVE-2023-6212, CVE-2023-6213)
It was discovered that Firefox did not properly manage memory when images were created on the canvas element. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6204)
It discovered that Firefox incorrectly handled certain memory when using a MessagePort. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6205)
It discovered that Firefox incorrectly did not properly manage ownership in ReadableByteStreams. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6207)
It discovered that Firefox incorrectly did not properly manage copy operations when using Selection API in X11. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6208)
Rachmat Abdul Rokhim discovered incorrectly handled parsing of relative URLS starting with '///'. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6209)

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-6509-2)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6509.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6509-2
url: https://launchpad.net/bugs/2045518
cve: CVE-2023-6204
cve: CVE-2023-6205
cve: CVE-2023-6206
cve: CVE-2023-6207
cve: CVE-2023-6208
cve: CVE-2023-6209
cve: CVE-2023-6210
cve: CVE-2023-6211
cve: CVE-2023-6212
cve: CVE-2023-6213
advisory_id: USN-6509-2
cert-bund: WID-SEC-2023-2995
dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-3078
dfn-cert: DFN-CERT-2023-2922
dfn-cert: DFN-CERT-2023-2920

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6562-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6562-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-121.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code.(CVE-2023-6865, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6866, CVE-2023-6867, CVE-2023-6861, CVE-2023-6869, CVE-2023-6871, CVE-2023-6872, CVE-2023-6863, CVE-2023-6864, CVE-2023-6873)
DoHyun Lee discovered that Firefox did not properly manage memory when used on systems with the Mesa VM driver. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2023-6856)
George Pantela and Hubert Kario discovered that Firefox using multiple NSS NIST curves which were susceptible to a side-channel attack known as 'Minerva'. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6135)
Andrew Osmond discovered that Firefox did not properly validate the textures produced by remote decoders. An attacker could potentially exploit this issue to escape the sandbox. (CVE-2023-6860)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6562-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6562.1
Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-6562-1`
`cve: CVE-2023-6135`
`cve: CVE-2023-6856`
`cve: CVE-2023-6857`
`cve: CVE-2023-6858`
`cve: CVE-2023-6859`
`cve: CVE-2023-6860`
`cve: CVE-2023-6861`
`cve: CVE-2023-6863`
`cve: CVE-2023-6864`
`cve: CVE-2023-6865`
`cve: CVE-2023-6866`
`cve: CVE-2023-6867`
`cve: CVE-2023-6869`
`cve: CVE-2023-6871`
`cve: CVE-2023-6872`
`cve: CVE-2023-6873`
`advisory_id: USN-6562-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2023-3185`
`dfn-cert: DFN-CERT-2024-1071`
`dfn-cert: DFN-CERT-2024-0955`
`dfn-cert: DFN-CERT-2024-0898`
`dfn-cert: DFN-CERT-2024-0491`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0369
dfn-cert: DFN-CERT-2024-0168
dfn-cert: DFN-CERT-2023-3181
dfn-cert: DFN-CERT-2023-3180

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6562-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6562-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-121.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6562-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code.(CVE-2023-6865, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6866, CVE-2023-6867, CVE-2023-6861, CVE-2023-6869, CVE-2023-6871, CVE-2023-6872, CVE-2023-6863, CVE-2023-6864, CVE-2023-6873)
DoHyun Lee discovered that Firefox did not properly manage memory when used on systems with the Mesa VM driver. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2023-6856)
George Pantela and Hubert Kario discovered that Firefox using multiple NSS NIST curves which were susceptible to a side-channel attack known as 'Minerva'. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6135)
Andrew Osmond discovered that Firefox did not properly validate the textures produced by remote decoders. An attacker could potentially exploit this issue to escape the sandbox. (CVE-2023-6860)

... 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-6562-2)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6562.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6562-2
url: https://launchpad.net/bugs/2048961
cve: CVE-2023-6135
cve: CVE-2023-6856
cve: CVE-2023-6857
cve: CVE-2023-6858
cve: CVE-2023-6859
cve: CVE-2023-6860
cve: CVE-2023-6861
cve: CVE-2023-6863
cve: CVE-2023-6864
cve: CVE-2023-6865
cve: CVE-2023-6866
cve: CVE-2023-6867
cve: CVE-2023-6869
cve: CVE-2023-6871
cve: CVE-2023-6872
cve: CVE-2023-6873
advisory_id: USN-6562-2
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-3185
dfn-cert: DFN-CERT-2024-1071
dfn-cert: DFN-CERT-2024-0955
dfn-cert: DFN-CERT-2024-0898
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0369
dfn-cert: DFN-CERT-2024-0168
dfn-cert: DFN-CERT-2023-3181
dfn-cert: DFN-CERT-2023-3180

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6610-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6610-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-122.0+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-0741, CVE-2024-0742, CVE-2024-0743, CVE-2024-0744, CVE-2024-0745, CVE-2024-0747, CVE-2024-0748, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0754, CVE-2024-0755)
Cornel Ionce discovered that Firefox did not properly manage memory when opening the print preview dialog. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-0746)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6610-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6610.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6610-1
cve: CVE-2024-0741
cve: CVE-2024-0742
cve: CVE-2024-0743
cve: CVE-2024-0744
cve: CVE-2024-0745
cve: CVE-2024-0746
cve: CVE-2024-0747
cve: CVE-2024-0748
cve: CVE-2024-0749
cve: CVE-2024-0750
cve: CVE-2024-0751
cve: CVE-2024-0753
cve: CVE-2024-0754
cve: CVE-2024-0755
advisory_id: USN-6610-1

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-0669
cert-bund: WID-SEC-2024-0185
dfn-cert: DFN-CERT-2024-1011
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-2024-0562
dfn-cert: DFN-CERT-2024-0188
dfn-cert: DFN-CERT-2024-0187

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6610-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6610-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-122.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6610-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
Original advisory details:

... continues on next page ...

... continued from previous page ...

Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-0741, CVE-2024-0742, CVE-2024-0743, CVE-2024-0744, CVE-2024-0745, CVE-2024-0747, CVE-2024-0748, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0754, CVE-2024-0755)
Cornel Ionce discovered that Firefox did not properly manage memory when opening the print preview dialog. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-0746)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6610-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6610.2
Version used: `2024-02-08T04:08:50Z`

References
`url: https://ubuntu.com/security/notices/USN-6610-2`
`url: https://launchpad.net/bugs/2052580`
`cve: CVE-2024-0741`
`cve: CVE-2024-0742`
`cve: CVE-2024-0743`
`cve: CVE-2024-0744`
`cve: CVE-2024-0745`
`cve: CVE-2024-0746`
`cve: CVE-2024-0747`
`cve: CVE-2024-0748`
`cve: CVE-2024-0749`
`cve: CVE-2024-0750`
`cve: CVE-2024-0751`
`cve: CVE-2024-0753`
`cve: CVE-2024-0754`
`cve: CVE-2024-0755`
`advisory_id: USN-6610-2`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0669`
`cert-bund: WID-SEC-2024-0185`
`dfn-cert: DFN-CERT-2024-1011`
`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-2024-0562`
`dfn-cert: DFN-CERT-2024-0188`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0187

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6433-1)

Summary
The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-6433-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: ghostscript
Installed version: ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version: >=ghostscript-9.50~dfsg-5ubuntu4.11

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

Affected Software/OS
'ghostscript' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled certain PDF documents. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6433-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6433.1
Version used: 2024-02-23T04:08:56Z

References
url: https://ubuntu.com/security/notices/USN-6433-1
cve: CVE-2023-43115
advisory_id: USN-6433-1
cert-bund: WID-SEC-2023-2380
dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-2368

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5686-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5686-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   git
Installed version:    git-1:2.25.1-1ubuntu3.1
Fixed version:      >=git-1:2.25.1-1ubuntu3.6
```

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

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

Vulnerability Insight
Cory Snider discovered that Git incorrectly handled certain symbolic links. An attacker could possibly use this issue to cause an unexpected behaviour. (CVE-2022-39253)
Kevin Backhouse discovered that Git incorrectly handled certain command strings. An attacker could possibly use this issue to arbitrary code execution. (CVE-2022-39260)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5686-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5686.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5686-1
cve: CVE-2022-39253
cve: CVE-2022-39260
advisory_id: USN-5686-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1981
cert-bund: WID-SEC-2022-1790
dfn-cert: DFN-CERT-2024-0228
dfn-cert: DFN-CERT-2023-0377
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2022-2848
dfn-cert: DFN-CERT-2022-2445
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2430
dfn-cert: DFN-CERT-2022-2353
dfn-cert: DFN-CERT-2022-2322

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5971-1)

Summary
The remote host is missing an update for the 'graphviz' package(s) announced via the USN-5971-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: graphviz
Installed version: graphviz-2.42.2-3build2
Fixed version: >=graphviz-2.42.2-3ubuntu0.1~esm1

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

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

Vulnerability Insight
It was discovered that graphviz contains null pointer dereference vulnerabilities. Exploitation via a specially crafted input file can cause a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-10196)
It was discovered that graphviz contains null pointer dereference vulnerabilities. Exploitation via a specially crafted input file can cause a denial of service. These issues only affected Ubuntu 14.04 ESM and Ubuntu 18.04 LTS. (CVE-2019-11023)
It was discovered that graphviz contains a buffer overflow vulnerability. Exploitation via a specially crafted input file can cause a denial of service or possibly allow for arbitrary code execution. These issues only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-18032)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5971-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5971.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5971-1

... continues on next page ...

... continued from previous page ...

cve: CVE-2018-10196
cve: CVE-2019-11023
cve: CVE-2020-18032
advisory_id: USN-5971-1
dfn-cert: DFN-CERT-2022-0266
dfn-cert: DFN-CERT-2021-1549
dfn-cert: DFN-CERT-2021-1033
dfn-cert: DFN-CERT-2021-1031
dfn-cert: DFN-CERT-2019-0825
dfn-cert: DFN-CERT-2018-0951

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5378-1)

Summary
The remote host is missing an update for the 'gzip' package(s) announced via the USN-5378-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: gzip
Installed version: gzip-1.10-0ubuntu4
Fixed version: >=gzip-1.10-0ubuntu4.1

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

Affected Software/OS
'gzip' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Cleemy Desu Wayo discovered that Gzip incorrectly handled certain filenames. If a user or automated system were tricked into performing zgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5378-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5378.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5378-1

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-1271
advisory_id: USN-5378-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0034
cert-bund: CB-K22/0407
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2115
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0788

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5156-1)

Summary
The remote host is missing an update for the 'icu' package(s) announced via the USN-5156-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: icu-devtools
Installed version: icu-devtools-66.1-2ubuntu2
Fixed version: >=icu-devtools-66.1-2ubuntu2.1
Vulnerable package: libicu-dev
Installed version: libicu-dev-66.1-2ubuntu2
Fixed version: >=libicu-dev-66.1-2ubuntu2.1
Vulnerable package: libicu66
Installed version: libicu66-66.1-2ubuntu2
Fixed version: >=libicu66-66.1-2ubuntu2.1

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'icu' package(s) on Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that ICU contains a double free issue. An attacker could 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-5156-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5156.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5156-1`
`cve: CVE-2021-30535`
`advisory_id: USN-5156-1`
`cert-bund: WID-SEC-2022-0487`
`cert-bund: CB-K21/0589`
`cert-bund: CB-K21/0578`
`dfn-cert: DFN-CERT-2022-0213`
`dfn-cert: DFN-CERT-2021-2470`
`dfn-cert: DFN-CERT-2021-1161`
`dfn-cert: DFN-CERT-2021-1138`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5953-1)

Summary
The remote host is missing an update for the 'ipython' package(s) announced via the USN-5953-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ipython3
Installed version:    ipython3-7.13.0-1
Fixed version:      >=ipython3-7.13.0-1ubuntu0.1~esm1
Vulnerable package:   python3-ipython
Installed version:    python3-ipython-7.13.0-1
Fixed version:      >=python3-ipython-7.13.0-1ubuntu0.1~esm1
```

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
It was discovered that IPython incorrectly processed REST API POST requests. An attacker could possibly use this issue to launch a cross-site request forgery (CSRF) attack and leak user's sensitive information. This issue only affected Ubuntu 14.04 ESM. (CVE-2015-5607)
It was discovered that IPython did not properly manage cross user temporary files. A local attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 18.04 ESM and Ubuntu 20.04 ESM. (CVE-2022-21699)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5953-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5953.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5953-1`
`cve: CVE-2015-5607`
`cve: CVE-2022-21699`
`advisory_id: USN-5953-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: CB-K15/1087`
`dfn-cert: DFN-CERT-2024-0089`
`dfn-cert: DFN-CERT-2022-0320`
`dfn-cert: DFN-CERT-2022-0173`
`dfn-cert: DFN-CERT-2015-1088`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6449-1)

Summary
The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-6449-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package: libavcodec58`
`Installed version: libavcodec58-7:4.2.4-1ubuntu0.1`

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=libavcodec58-7:4.2.7-0ubuntu0.1+esm3
Vulnerable package:   libavformat58
Installed version:    libavformat58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavformat58-7:4.2.7-0ubuntu0.1+esm3
Vulnerable package:   libavutil56
Installed version:    libavutil56-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavutil56-7:4.2.7-0ubuntu0.1+esm3
Vulnerable package:   libpostproc55
Installed version:    libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version:      >=libpostproc55-7:4.2.7-0ubuntu0.1+esm3
Vulnerable package:   libswresample3
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1+esm3
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1+esm3
```

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

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

Vulnerability Insight
It was discovered that FFmpeg incorrectly managed memory resulting in a memory leak. An attacker could possibly use this issue to cause a denial of service via application crash. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-22038)
It was discovered that FFmpeg incorrectly handled certain input files, leading to an integer overflow. An attacker could possibly use this issue to cause a denial of service via application crash. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-20898, CVE-2021-38090, CVE-2021-38091, CVE-2021-38092, CVE-2021-38093, CVE-2021-38094)
It was discovered that FFmpeg incorrectly managed memory, resulting in a memory leak. If a user or automated system were tricked into processing a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2022-48434)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6449-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6449.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6449-1`
`cve: CVE-2020-20898`

... continues on next page ...

... continued from previous page ...

cve: CVE-2020-22038
cve: CVE-2021-38090
cve: CVE-2021-38091
cve: CVE-2021-38092
cve: CVE-2021-38093
cve: CVE-2021-38094
cve: CVE-2022-48434
advisory_id: USN-6449-1
cert-bund: WID-SEC-2023-0792
cert-bund: WID-SEC-2023-0011
cert-bund: WID-SEC-2023-0009
cert-bund: CB-K21/0998
cert-bund: CB-K21/0599
dfn-cert: DFN-CERT-2024-1134
dfn-cert: DFN-CERT-2023-2604
dfn-cert: DFN-CERT-2023-1028
dfn-cert: DFN-CERT-2023-0789
dfn-cert: DFN-CERT-2023-0719
dfn-cert: DFN-CERT-2023-0013
dfn-cert: DFN-CERT-2021-2242
dfn-cert: DFN-CERT-2021-1863
dfn-cert: DFN-CERT-2021-1502

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6449-2)

Summary
The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-6449-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libavcodec58
Installed version: libavcodec58-7:4.2.4-1ubuntu0.1
Fixed version: >=libavcodec58-7:4.2.7-0ubuntu0.1+esm4
Vulnerable package: libavformat58
Installed version: libavformat58-7:4.2.4-1ubuntu0.1
Fixed version: >=libavformat58-7:4.2.7-0ubuntu0.1+esm4
Vulnerable package: libavutil56
Installed version: libavutil56-7:4.2.4-1ubuntu0.1
Fixed version: >=libavutil56-7:4.2.7-0ubuntu0.1+esm4
Vulnerable package: libpostproc55
Installed version: libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version: >=libpostproc55-7:4.2.7-0ubuntu0.1+esm4
Vulnerable package: libswresample3

... continues on next page ...

... continued from previous page ...

```
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1+esm4
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1+esm4
```

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

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

Vulnerability Insight
USN-6449-1 fixed vulnerabilities in FFmpeg. Unfortunately that update could introduce a regression in tools using an FFmpeg library, like VLC.
This updated fixes the problem. We apologize for the inconvenience.
Original advisory details:
It was discovered that FFmpeg incorrectly managed memory resulting in a memory leak. An attacker could possibly use this issue to cause a denial of service via application crash. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-22038)
It was discovered that FFmpeg incorrectly handled certain input files, leading to an integer overflow. An attacker could possibly use this issue to cause a denial of service via application crash. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-20898, CVE-2021-38090, CVE-2021-38091, CVE-2021-38092, CVE-2021-38093, CVE-2021-38094)
It was discovered that FFmpeg incorrectly managed memory, resulting in a memory leak. If a user or automated system were tricked into processing a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service, or execute arbitrary code. (CVE-2022-48434)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6449-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6449.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6449-2`
`url: https://launchpad.net/bugs/2042743`
`cve: CVE-2020-20898`
`cve: CVE-2020-22038`
`cve: CVE-2021-38090`
`cve: CVE-2021-38091`
`cve: CVE-2021-38092`
`cve: CVE-2021-38093`
`cve: CVE-2021-38094`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-48434
advisory_id: USN-6449-2
cert-bund: WID-SEC-2023-0792
cert-bund: WID-SEC-2023-0011
cert-bund: WID-SEC-2023-0009
cert-bund: CB-K21/0998
cert-bund: CB-K21/0599
dfn-cert: DFN-CERT-2024-1134
dfn-cert: DFN-CERT-2023-2604
dfn-cert: DFN-CERT-2023-1028
dfn-cert: DFN-CERT-2023-0789
dfn-cert: DFN-CERT-2023-0719
dfn-cert: DFN-CERT-2023-0013
dfn-cert: DFN-CERT-2021-2242
dfn-cert: DFN-CERT-2021-1863
dfn-cert: DFN-CERT-2021-1502
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6423-1)

Summary
The remote host is missing an update for the 'libcue' package(s) announced via the USN-6423-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libcue2
Installed version:    libcue2-2.2.1-2
Fixed version:      >=libcue2-2.2.1-2ubuntu0.1
```

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

Affected Software/OS
'libcue' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that CUE incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6423-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2023.6423.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6423-1
cve: CVE-2023-43641
advisory_id: USN-6423-1
cert-bund: WID-SEC-2023-2601
dfn-cert: DFN-CERT-2023-2434

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5154-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-5154-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libfreerdp-client2-2
Installed version: libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version: >=libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.2

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

Affected Software/OS
'freerdp2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-41159)
It was discovered that FreeRDP incorrectly handled certain connections. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2021-41160)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5154-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5154.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5154-1

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-41159
cve: CVE-2021-41160
advisory_id: USN-5154-1
cert-bund: WID-SEC-2022-0278
cert-bund: CB-K21/1198
dfn-cert: DFN-CERT-2023-2897
dfn-cert: DFN-CERT-2021-2396

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5607-1)

Summary
The remote host is missing an update for the 'gdk-pixbuf' package(s) announced via the USN-5607-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgdk-pixbuf2.0-0
Installed version: libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.2
Fixed version: >=libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.4

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

Affected Software/OS
'gdk-pixbuf' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that GDK-PixBuf incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5607-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5607.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5607-1
cve: CVE-2021-44648
advisory_id: USN-5607-1
cert-bund: WID-SEC-2023-1185
dfn-cert: DFN-CERT-2022-1996

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0269

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5828-1)

Summary
The remote host is missing an update for the 'krb5' package(s) announced via the USN-5828-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgssapi-krb5-2
Installed version: libgssapi-krb5-2-1.17-6ubuntu4.1
Fixed version: >=libgssapi-krb5-2-1.17-6ubuntu4.2

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

Affected Software/OS
'krb5' 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 Kerberos incorrectly handled certain S4U2Self requests. An attacker could possibly use this issue to cause a denial of service. This issue was only addressed in Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2018-20217)
Greg Hudson discovered that Kerberos PAC implementation incorrectly handled certain parsing operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-42898)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5828-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5828.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5828-1
cve: CVE-2018-20217
cve: CVE-2022-42898
advisory_id: USN-5828-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2690

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0199
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2057
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K19/0013
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2657
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2022-2579
dfn-cert: DFN-CERT-2021-2044
dfn-cert: DFN-CERT-2019-0362
dfn-cert: DFN-CERT-2019-0176
dfn-cert: DFN-CERT-2018-2619
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5024-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5024-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.32.3-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.32.3-0ubuntu0.20.04.1
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
A large number of 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-5024-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5024.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5024-1`
`cve: CVE-2021-21775`
`cve: CVE-2021-21779`
`cve: CVE-2021-30663`
`cve: CVE-2021-30665`
`cve: CVE-2021-30689`
`cve: CVE-2021-30720`
`cve: CVE-2021-30734`
`cve: CVE-2021-30744`
`cve: CVE-2021-30749`
`cve: CVE-2021-30758`
`cve: CVE-2021-30795`
`cve: CVE-2021-30797`
`cve: CVE-2021-30799`
`advisory_id: USN-5024-1`
`cert-bund: CB-K21/0795`
`cert-bund: CB-K21/0794`
`cert-bund: CB-K21/0792`
`cert-bund: CB-K21/0573`
`cert-bund: CB-K21/0572`
`cert-bund: CB-K21/0565`
`cert-bund: CB-K21/0474`
`cert-bund: CB-K21/0468`
`cert-bund: CB-K21/0467`
`dfn-cert: DFN-CERT-2021-2392`
`dfn-cert: DFN-CERT-2021-1728`
`dfn-cert: DFN-CERT-2021-1599`
`dfn-cert: DFN-CERT-2021-1587`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1578
dfn-cert: DFN-CERT-2021-1577
dfn-cert: DFN-CERT-2021-1576
dfn-cert: DFN-CERT-2021-1575
dfn-cert: DFN-CERT-2021-1132
dfn-cert: DFN-CERT-2021-1129
dfn-cert: DFN-CERT-2021-1128
dfn-cert: DFN-CERT-2021-0941
dfn-cert: DFN-CERT-2021-0928
dfn-cert: DFN-CERT-2021-0927
dfn-cert: DFN-CERT-2021-0926

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5087-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5087-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.32.4-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.32.4-0ubuntu0.20.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
A large number of 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-5087-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2021.5087.1
Version used: 2024-02-02T04:09:01Z

References

```
url: https://ubuntu.com/security/notices/USN-5087-1
cve: CVE-2021-30858
advisory_id: USN-5087-1
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1210
cert-bund: CB-K21/1007
cert-bund: CB-K21/0994
cert-bund: CB-K21/0958
cert-bund: CB-K21/0957
cert-bund: CB-K21/0956
dfn-cert: DFN-CERT-2022-0191
dfn-cert: DFN-CERT-2022-0190
dfn-cert: DFN-CERT-2022-0154
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2228
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2060
dfn-cert: DFN-CERT-2021-2000
dfn-cert: DFN-CERT-2021-1960
dfn-cert: DFN-CERT-2021-1918
dfn-cert: DFN-CERT-2021-1916
dfn-cert: DFN-CERT-2021-1915
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5127-1)

Summary

The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5127-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.34.1-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.34.1-0ubuntu0.20.04.1
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
A large number of 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-5127-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5127.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5127-1`
`cve: CVE-2021-30846`
`cve: CVE-2021-30851`
`cve: CVE-2021-42762`
`advisory_id: USN-5127-1`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K21/0996`
`cert-bund: CB-K21/0993`
`dfn-cert: DFN-CERT-2022-1051`
`dfn-cert: DFN-CERT-2022-0369`
`dfn-cert: DFN-CERT-2022-0191`
`dfn-cert: DFN-CERT-2022-0190`
`dfn-cert: DFN-CERT-2022-0154`
`dfn-cert: DFN-CERT-2021-2514`
`dfn-cert: DFN-CERT-2021-2293`
`dfn-cert: DFN-CERT-2021-2269`
`dfn-cert: DFN-CERT-2021-2234`
`dfn-cert: DFN-CERT-2021-2228`
`dfn-cert: DFN-CERT-2021-1967`
`dfn-cert: DFN-CERT-2021-1965`
`dfn-cert: DFN-CERT-2021-1918`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5255-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5255-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.34.4-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.34.4-0ubuntu0.20.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
A large number of 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-5255-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5255.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5255-1
cve: CVE-2021-30934
cve: CVE-2021-30936
cve: CVE-2021-30951
cve: CVE-2021-30952
cve: CVE-2021-30953
cve: CVE-2021-30954
cve: CVE-2021-30984
advisory_id: USN-5255-1
cert-bund: WID-SEC-2022-1335
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0489
cert-bund: CB-K21/1273
cert-bund: CB-K21/1272
dfn-cert: DFN-CERT-2022-1051
dfn-cert: DFN-CERT-2022-0493
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0164
dfn-cert: DFN-CERT-2021-2615
dfn-cert: DFN-CERT-2021-2591
dfn-cert: DFN-CERT-2021-2590
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5306-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5306-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.34.6-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.34.6-0ubuntu0.20.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
A large number of 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-5306-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2022.5306.1
Version used: 2024-02-02T04:09:01Z

References

```
url: https://ubuntu.com/security/notices/USN-5306-1
cve: CVE-2022-22589
cve: CVE-2022-22590
cve: CVE-2022-22592
advisory_id: USN-5306-1
cert-bund: WID-SEC-2023-1213
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1057
cert-bund: CB-K22/0619
cert-bund: CB-K22/0112
cert-bund: CB-K22/0111
cert-bund: CB-K22/0108
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1051
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0493
dfn-cert: DFN-CERT-2022-0408
dfn-cert: DFN-CERT-2022-0324
dfn-cert: DFN-CERT-2022-0202
dfn-cert: DFN-CERT-2022-0199
dfn-cert: DFN-CERT-2022-0198
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5394-1)

Summary

The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5394-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.0-0ubuntu0.20.04.3
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.36.0-0ubuntu0.20.04.3
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
A large number of 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-5394-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5394.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5394-1`
`cve: CVE-2022-22624`
`cve: CVE-2022-22628`
`cve: CVE-2022-22629`
`cve: CVE-2022-22637`
`advisory_id: USN-5394-1`
`cert-bund: WID-SEC-2022-2044`
`cert-bund: WID-SEC-2022-1056`
`cert-bund: CB-K22/0317`
`cert-bund: CB-K22/0316`
`cert-bund: CB-K22/0315`
`dfn-cert: DFN-CERT-2022-2513`
`dfn-cert: DFN-CERT-2022-1051`
`dfn-cert: DFN-CERT-2022-0991`
`dfn-cert: DFN-CERT-2022-0942`
`dfn-cert: DFN-CERT-2022-0786`
`dfn-cert: DFN-CERT-2022-0605`
`dfn-cert: DFN-CERT-2022-0590`
`dfn-cert: DFN-CERT-2022-0589`
`dfn-cert: DFN-CERT-2022-0586`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5457-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5457-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.3-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.36.3-0ubuntu0.20.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
A large number of 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-5457-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5457.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5457-1
cve: CVE-2022-26700
cve: CVE-2022-26709
cve: CVE-2022-26716
cve: CVE-2022-26717
cve: CVE-2022-26719
advisory_id: USN-5457-1
cert-bund: WID-SEC-2022-2044
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0541
cert-bund: WID-SEC-2022-0339
cert-bund: CB-K22/0627
cert-bund: CB-K22/0620
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0619
cert-bund: CB-K22/0617
dfn-cert: DFN-CERT-2022-2513
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1224
dfn-cert: DFN-CERT-2022-1136
dfn-cert: DFN-CERT-2022-1120
dfn-cert: DFN-CERT-2022-1117
dfn-cert: DFN-CERT-2022-1116

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5522-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5522-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libjavascriptcoregtk-4.0-18
Installed version: libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libjavascriptcoregtk-4.0-18-2.36.4-0ubuntu0.20.04.1
Vulnerable package: libwebkit2gtk-4.0-37
Installed version: libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libwebkit2gtk-4.0-37-2.36.4-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Several security issues were discovered in 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-5522-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5522.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5522-1
cve: CVE-2022-22677
cve: CVE-2022-26710
advisory_id: USN-5522-1
cert-bund: WID-SEC-2022-2044
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0339
cert-bund: CB-K22/0619
cert-bund: CB-K22/0617
dfn-cert: DFN-CERT-2022-2513
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1499
dfn-cert: DFN-CERT-2022-1117
dfn-cert: DFN-CERT-2022-1116

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5568-1)

Summary

The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5568-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.6-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.36.6-0ubuntu0.20.04.1
```

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

Affected Software/OS

'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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-5568-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5568.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5568-1`
`cve: CVE-2022-2294`
`cve: CVE-2022-32792`
`cve: CVE-2022-32816`
`advisory_id: USN-5568-1`
`cert-bund: WID-SEC-2022-0782`
`cert-bund: WID-SEC-2022-0780`
`cert-bund: WID-SEC-2022-0778`
`cert-bund: WID-SEC-2022-0592`
`cert-bund: WID-SEC-2022-0556`
`dfn-cert: DFN-CERT-2022-1825`
`dfn-cert: DFN-CERT-2022-1681`
`dfn-cert: DFN-CERT-2022-1635`
`dfn-cert: DFN-CERT-2022-1633`
`dfn-cert: DFN-CERT-2022-1631`
`dfn-cert: DFN-CERT-2022-1599`
`dfn-cert: DFN-CERT-2022-1574`
`dfn-cert: DFN-CERT-2022-1552`
`dfn-cert: DFN-CERT-2022-1494`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5611-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5611-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.7-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
```

... continues on next page ...

... continued from previous page ...

Installed version: libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libwebkit2gtk-4.0-37-2.36.7-0ubuntu0.20.04.1

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

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

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-5611-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5611.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5611-1
cve: CVE-2022-32893
advisory_id: USN-5611-1
cert-bund: WID-SEC-2022-1078
cert-bund: WID-SEC-2022-1071
cert-bund: WID-SEC-2022-1070
dfn-cert: DFN-CERT-2022-1916
dfn-cert: DFN-CERT-2022-1886
dfn-cert: DFN-CERT-2022-1845
dfn-cert: DFN-CERT-2022-1840
dfn-cert: DFN-CERT-2022-1839

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5642-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5642-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.8-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.36.8-0ubuntu0.20.04.1
```

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

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

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-5642-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5642.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5642-1
cve: CVE-2022-32886
advisory_id: USN-5642-1
cert-bund: WID-SEC-2023-1185
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1394
cert-bund: WID-SEC-2022-1389
dfn-cert: DFN-CERT-2023-1055
dfn-cert: DFN-CERT-2023-0979
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2065
dfn-cert: DFN-CERT-2022-2005
dfn-cert: DFN-CERT-2022-2004
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5730-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5730-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.2-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.2-0ubuntu0.20.04.1
```

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-5730-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5730.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5730-1
cve: CVE-2022-32888
cve: CVE-2022-32923
cve: CVE-2022-42799
cve: CVE-2022-42823
cve: CVE-2022-42824
advisory_id: USN-5730-1
cert-bund: WID-SEC-2023-1185
cert-bund: WID-SEC-2022-1888
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1841
cert-bund: WID-SEC-2022-1837
dfn-cert: DFN-CERT-2023-1055
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2525
dfn-cert: DFN-CERT-2022-2477
dfn-cert: DFN-CERT-2022-2415
dfn-cert: DFN-CERT-2022-2367
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2363

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5797-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5797-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.3-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.3-0ubuntu0.20.04.1
```

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-5797-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5797.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5797-1`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-42852
cve: CVE-2022-42856
cve: CVE-2022-42867
cve: CVE-2022-46692
cve: CVE-2022-46698
cve: CVE-2022-46699
cve: CVE-2022-46700
advisory_id: USN-5797-1
cert-bund: WID-SEC-2023-1185
cert-bund: WID-SEC-2023-0022
cert-bund: WID-SEC-2022-2321
cert-bund: WID-SEC-2022-2314
cert-bund: WID-SEC-2022-2313
dfn-cert: DFN-CERT-2023-1055
dfn-cert: DFN-CERT-2023-0448
dfn-cert: DFN-CERT-2022-2930
dfn-cert: DFN-CERT-2022-2908
dfn-cert: DFN-CERT-2022-2844
dfn-cert: DFN-CERT-2022-2843
dfn-cert: DFN-CERT-2022-2840
dfn-cert: DFN-CERT-2022-2839
dfn-cert: DFN-CERT-2022-2838
dfn-cert: DFN-CERT-2022-2837

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libjavascriptcoregtk-4.0-18
Installed version: libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libjavascriptcoregtk-4.0-18-2.38.4-0ubuntu0.20.04.2
Vulnerable package: libwebkit2gtk-4.0-37
Installed version: libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libwebkit2gtk-4.0-37-2.38.4-0ubuntu0.20.04.2

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: `2024-02-02T04:09:01Z`

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-2023-1185`
`cert-bund: WID-SEC-2023-0190`
`cert-bund: WID-SEC-2023-0189`
`cert-bund: WID-SEC-2023-0181`
`dfn-cert: DFN-CERT-2023-1055`
`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.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.5-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.5-0ubuntu0.20.04.1
```

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: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5893-1
cve: CVE-2023-23529
advisory_id: USN-5893-1
cert-bund: WID-SEC-2023-0778
cert-bund: WID-SEC-2023-0358
cert-bund: WID-SEC-2023-0355
cert-bund: WID-SEC-2023-0347
dfn-cert: DFN-CERT-2023-0684
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: 8.8)
NVT: Ubuntu: Security Advisory (USN-6061-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-6061-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libjavascriptcoregtk-4.0-18
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.38.6-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.38.6-0ubuntu0.20.04.1
```

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, Ubuntu 23.04.

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-6061-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6061.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6061-1
cve: CVE-2022-0108
cve: CVE-2022-32885
cve: CVE-2023-25358
cve: CVE-2023-27932
cve: CVE-2023-27954
cve: CVE-2023-28205
advisory_id: USN-6061-1
cert-bund: WID-SEC-2023-1185
cert-bund: WID-SEC-2023-0910
cert-bund: WID-SEC-2023-0778
cert-bund: WID-SEC-2023-0777
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0770
cert-bund: WID-SEC-2022-0782
cert-bund: WID-SEC-2022-0778
cert-bund: CB-K22/0007
cert-bund: CB-K22/0004
dfn-cert: DFN-CERT-2023-2766
dfn-cert: DFN-CERT-2023-1055
dfn-cert: DFN-CERT-2023-0979
dfn-cert: DFN-CERT-2023-0932
dfn-cert: DFN-CERT-2023-0931
dfn-cert: DFN-CERT-2023-0786
dfn-cert: DFN-CERT-2023-0785
dfn-cert: DFN-CERT-2023-0784
dfn-cert: DFN-CERT-2023-0688
dfn-cert: DFN-CERT-2023-0685
dfn-cert: DFN-CERT-2023-0684
dfn-cert: DFN-CERT-2023-0683
dfn-cert: DFN-CERT-2023-0327
dfn-cert: DFN-CERT-2022-0419
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0025
dfn-cert: DFN-CERT-2022-0011

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5631-1)

Summary
The remote host is missing an update for the 'libjpeg-turbo' package(s) announced via the USN-5631-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libjpeg-turbo8
Installed version: libjpeg-turbo8-2.0.3-0ubuntu1.20.04.1
Fixed version: >=libjpeg-turbo8-2.0.3-0ubuntu1.20.04.3

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

Affected Software/OS
'libjpeg-turbo' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that libjpeg-turbo incorrectly handled certain EOF characters. An attacker could possibly use this issue to cause libjpeg-turbo to consume resource, leading to a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-11813)
It was discovered that libjpeg-turbo incorrectly handled certain malformed jpeg files. An attacker could possibly use this issue to cause libjpeg-turbo to crash, resulting in a denial of service. (CVE-2020-17541, CVE-2020-35538)
It was discovered that libjpeg-turbo incorrectly handled certain malformed PPM files. An attacker could use this issue to cause libjpeg-turbo to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-46822)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5631-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5631.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5631-1`
`cve: CVE-2018-11813`
`cve: CVE-2020-17541`
`cve: CVE-2020-35538`
`cve: CVE-2021-46822`
`advisory_id: USN-5631-1`
`cert-bund: WID-SEC-2023-0576`
`cert-bund: WID-SEC-2022-0571`
`cert-bund: WID-SEC-2022-0517`
`cert-bund: CB-K21/1164`
`cert-bund: CB-K19/0696`
`dfn-cert: DFN-CERT-2023-0501`
`dfn-cert: DFN-CERT-2022-2198`
`dfn-cert: DFN-CERT-2022-2117`
`dfn-cert: DFN-CERT-2022-1751`
`dfn-cert: DFN-CERT-2022-1460`
`dfn-cert: DFN-CERT-2021-1280`
`dfn-cert: DFN-CERT-2019-1615`
`dfn-cert: DFN-CERT-2019-0590`
`dfn-cert: DFN-CERT-2018-1243`
`dfn-cert: DFN-CERT-2018-1168`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6099-1)

Summary
The remote host is missing an update for the 'ncurses' package(s) announced via the USN-6099-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libncurses6
Installed version:    libncurses6-6.2-0ubuntu2
Fixed version:      >=libncurses6-6.2-0ubuntu2.1
Vulnerable package:   libncursesw6
Installed version:    libncursesw6-6.2-0ubuntu2
Fixed version:      >=libncursesw6-6.2-0ubuntu2.1
Vulnerable package:   libtinfo6
Installed version:    libtinfo6-6.2-0ubuntu2
Fixed version:      >=libtinfo6-6.2-0ubuntu2.1
Vulnerable package:   ncurses-bin
Installed version:    ncurses-bin-6.2-0ubuntu2
Fixed version:      >=ncurses-bin-6.2-0ubuntu2.1
```

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

Affected Software/OS
'ncurses' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that ncurses was incorrectly performing bounds checks when processing invalid hashcodes. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-17594)
It was discovered that ncurses was incorrectly handling end-of-string characters when processing terminfo and termcap files. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-17595)
It was discovered that ncurses was incorrectly handling end-of-string characters when converting between termcap and terminfo formats. 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 and Ubuntu 20.04 LTS. (CVE-2021-39537)
It was discovered that ncurses was incorrectly performing bounds checks when dealing with corrupt terminfo data while reading a terminfo file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-29458)
It was discovered that ncurses was parsing environment variables when running with setuid applications and not properly handling the processing of malformed data when doing so. A local attacker could possibly use this issue to cause a denial of service (application crash) or execute arbitrary code. (CVE-2023-29491)

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-6099-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6099.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6099-1
cve: CVE-2019-17594
cve: CVE-2019-17595
cve: CVE-2021-39537
cve: CVE-2022-29458
cve: CVE-2023-29491
advisory_id: USN-6099-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2390
cert-bund: WID-SEC-2023-1098
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-0571
cert-bund: CB-K21/1164
dfn-cert: DFN-CERT-2024-0112
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-3027
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1700
dfn-cert: DFN-CERT-2023-1186
dfn-cert: DFN-CERT-2023-1033
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-1765
dfn-cert: DFN-CERT-2022-1326
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2209
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2529
dfn-cert: DFN-CERT-2019-2438

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5506-1)

Summary

The remote host is missing an update for the 'nss' package(s) announced via the USN-5506-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.49.1-1ubuntu1.5
Fixed version:      >=libnss3-2:3.49.1-1ubuntu1.8
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Tavis Ormandy discovered that NSS incorrectly handled an empty pkcs7 sequence. A remote attacker could possibly use this issue to cause NSS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. (CVE-2022-22747) Ronald Crane discovered that NSS incorrectly handled certain memory operations. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-34480)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5506-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5506.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5506-1
cve: CVE-2022-22747
cve: CVE-2022-34480
advisory_id: USN-5506-1
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2022-1251
cert-bund: WID-SEC-2022-0611
cert-bund: WID-SEC-2022-0505
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K22/0039
dfn-cert: DFN-CERT-2022-1524
dfn-cert: DFN-CERT-2022-1440
dfn-cert: DFN-CERT-2022-0452
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0187
dfn-cert: DFN-CERT-2022-0068
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0046
dfn-cert: DFN-CERT-2022-0045

High (CVSS: 8.8)
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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libnss3
Installed version: libnss3-2:3.49.1-1ubuntu1.5
Fixed version: >=libnss3-2:3.49.1-1ubuntu1.9

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)
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: 2024-02-02T04:09:01Z

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-2024-0120
cert-bund: WID-SEC-2024-0064

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0407
cert-bund: WID-SEC-2023-0385
cert-bund: WID-SEC-2022-1708
dfn-cert: DFN-CERT-2024-0125
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0843
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: 8.8)
NVT: Ubuntu: Security Advisory (USN-5718-1)

Summary
The remote host is missing an update for the 'pixman' package(s) announced via the USN-5718-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpixman-1-0
Installed version: libpixman-1-0-0.38.4-0ubuntu1
Fixed version: >=libpixman-1-0-0.38.4-0ubuntu2.1

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

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

Vulnerability Insight
Maddie Stone discovered that pixman incorrectly handled certain memory operations. A remote attacker could use this issue to cause pixman to crash, resulting in 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-5718-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2022.5718.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5718-1
cve: CVE-2022-44638
advisory_id: USN-5718-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2994
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-2372
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2022-2488
dfn-cert: DFN-CERT-2022-2480

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5025-1)

Summary
The remote host is missing an update for the 'libsndfile' package(s) announced via the USN-5025-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libsndfile1
Installed version: libsndfile1-1.0.28-7
Fixed version: >=libsndfile1-1.0.28-7ubuntu0.1

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

Affected Software/OS
'libsndfile' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in 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-5025-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5025.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5025-1
cve: CVE-2021-3246
advisory_id: USN-5025-1
cert-bund: WID-SEC-2023-2522
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1667
dfn-cert: DFN-CERT-2021-1616

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5743-2)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5743-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.7

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

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

Vulnerability Insight
USN-5743-1 fixed a vulnerability in LibTIFF. This update provides the corresponding updates for Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10.
Original advisory details:
It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5743-2)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2022.5743.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5743-2
cve: CVE-2022-3970
advisory_id: USN-5743-2
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-2035
dfn-cert: DFN-CERT-2023-1700
dfn-cert: DFN-CERT-2023-1124
dfn-cert: DFN-CERT-2023-1050
dfn-cert: DFN-CERT-2023-0141
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2022-2695
dfn-cert: DFN-CERT-2022-2680

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6403-1)

Summary
The remote host is missing an update for the 'libvpx' package(s) announced via the USN-6403-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libvpx6
Installed version: libvpx6-1.8.2-1build1
Fixed version: >=libvpx6-1.8.2-1ubuntu0.2

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

Affected Software/OS
'libvpx' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that libvpx did not properly handle certain malformed media files. If an application using libvpx opened a specially crafted file, a remote attacker could cause a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6403-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6403.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6403-1
cve: CVE-2023-44488
cve: CVE-2023-5217
advisory_id: USN-6403-1
cert-bund: WID-SEC-2023-2599
cert-bund: WID-SEC-2023-2572
cert-bund: WID-SEC-2023-2514
cert-bund: WID-SEC-2023-2498
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2816
dfn-cert: DFN-CERT-2023-2799
dfn-cert: DFN-CERT-2023-2698
dfn-cert: DFN-CERT-2023-2673
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2484
dfn-cert: DFN-CERT-2023-2435
dfn-cert: DFN-CERT-2023-2433
dfn-cert: DFN-CERT-2023-2408
dfn-cert: DFN-CERT-2023-2397
dfn-cert: DFN-CERT-2023-2395
dfn-cert: DFN-CERT-2023-2384
dfn-cert: DFN-CERT-2023-2358
dfn-cert: DFN-CERT-2023-2357
dfn-cert: DFN-CERT-2023-2348
dfn-cert: DFN-CERT-2023-2344
dfn-cert: DFN-CERT-2023-2330
dfn-cert: DFN-CERT-2023-2310

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6369-1)

Summary

The remote host is missing an update for the 'libwebp' package(s) announced via the USN-6369-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: libwebp6
Installed version: libwebp6-0.6.1-2ubuntu0.20.04.1

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=libwebp6-0.6.1-2ubuntu0.20.04.3
Vulnerable package:   libwebpdemux2
Installed version:    libwebpdemux2-0.6.1-2ubuntu0.20.04.1
Fixed version:      >=libwebpdemux2-0.6.1-2ubuntu0.20.04.3
Vulnerable package:   libwebpmux3
Installed version:    libwebpmux3-0.6.1-2ubuntu0.20.04.1
Fixed version:      >=libwebpmux3-0.6.1-2ubuntu0.20.04.3
```

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

Affected Software/OS
'libwebp' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that libwebp incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in 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-6369-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6369.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6369-1
cve: CVE-2023-4863
advisory_id: USN-6369-1
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-3099
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2841
cert-bund: WID-SEC-2023-2548
cert-bund: WID-SEC-2023-2538
cert-bund: WID-SEC-2023-2313
cert-bund: WID-SEC-2023-2310
cert-bund: WID-SEC-2023-2305
dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2356
dfn-cert: DFN-CERT-2023-2325
dfn-cert: DFN-CERT-2023-2303
dfn-cert: DFN-CERT-2023-2283
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2282
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2176
dfn-cert: DFN-CERT-2023-2152
dfn-cert: DFN-CERT-2023-2149
dfn-cert: DFN-CERT-2023-2120
dfn-cert: DFN-CERT-2023-2119
dfn-cert: DFN-CERT-2023-2110

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5807-1)

Summary
The remote host is missing an update for the 'libxpm' package(s) announced via the USN-5807-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libxpm4
Installed version: libxpm4-1:3.5.12-1
Fixed version: >=libxpm4-1:3.5.12-1ubuntu0.20.04.1

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

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

Vulnerability Insight
Martin Ettl discovered that libXpm incorrectly handled certain XPM files. If a user or automated system were tricked into opening a specially crafted XPM file, a remote attacker could possibly use this issue to cause libXpm to stop responding, resulting in a denial of service. (CVE-2022-44617)
Marco Ivaldi discovered that libXpm incorrectly handled certain XPM files. If a user or automated system were tricked into opening a specially crafted XPM file, a remote attacker could possibly use this issue to cause libXpm to stop responding, resulting in a denial of service. (CVE-2022-46285)
Alan Coopersmith discovered that libXpm incorrectly handled calling external helper binaries. If libXpm was being used by a setuid binary, a local attacker could possibly use this issue to escalate privileges. (CVE-2022-4883)

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-5807-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5807.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5807-1
cve: CVE-2022-44617
cve: CVE-2022-46285
cve: CVE-2022-4883
advisory_id: USN-5807-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0113
dfn-cert: DFN-CERT-2023-1714
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0107

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5575-1)

Summary
The remote host is missing an update for the 'libxslt' package(s) announced via the USN-5575-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libxslt1.1
Installed version: libxslt1.1-1.1.34-4
Fixed version: >=libxslt1.1-1.1.34-4ubuntu0.20.04.1

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

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

Vulnerability Insight
Nicolas Gregoire discovered that Libxslt incorrectly handled certain XML. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-5815)
Alexey Neyman incorrectly handled certain HTML pages. An attacker could possibly use this issue to expose sensitive information or execute arbitrary code. (CVE-2021-30560)

... 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-5575-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5575.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5575-1
cve: CVE-2019-5815
cve: CVE-2021-30560
advisory_id: USN-5575-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2022-1173
cert-bund: WID-SEC-2022-1117
cert-bund: WID-SEC-2022-1088
cert-bund: CB-K21/0800
cert-bund: CB-K21/0762
cert-bund: CB-K19/0341
dfn-cert: DFN-CERT-2022-1880
dfn-cert: DFN-CERT-2022-1857
dfn-cert: DFN-CERT-2022-1669
dfn-cert: DFN-CERT-2022-1599
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2021-1511
dfn-cert: DFN-CERT-2019-1785
dfn-cert: DFN-CERT-2019-1318
dfn-cert: DFN-CERT-2019-1317
dfn-cert: DFN-CERT-2019-0822

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5071-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5071-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.84.88

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Maxim Levitsky and Paolo Bonzini discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel allowed a guest VM to disable restrictions on VMLOAD/VMSAVE in a nested guest. An attacker in a guest VM could use this to read or write portions of the host's physical memory. (CVE-2021-3656)
Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. (CVE-2021-3653)
It was discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not ensure enough processing time was given to perform cleanups of large SEV VMs. A local attacker could use this to cause a denial of service (soft lockup). (CVE-2020-36311)
It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. An attacker who could start and control a VM could possibly use this to expose sensitive information or execute arbitrary code. (CVE-2021-22543)
Murray McAllister discovered that the joystick device interface in the Linux kernel did not properly validate data passed via an ioctl(). A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code on systems with a joystick device registered. (CVE-2021-3612)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5071-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5071.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5071-1`
`cve: CVE-2020-36311`
`cve: CVE-2021-22543`
`cve: CVE-2021-3612`
`cve: CVE-2021-3653`
`cve: CVE-2021-3656`
`advisory_id: USN-5071-1`
`cert-bund: WID-SEC-2023-0063`
`cert-bund: WID-SEC-2022-2072`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-2065
cert-bund: WID-SEC-2022-0243
cert-bund: WID-SEC-2022-0242
cert-bund: WID-SEC-2022-0213
cert-bund: CB-K21/0879
cert-bund: CB-K21/0849
cert-bund: CB-K21/0729
cert-bund: CB-K21/0696
cert-bund: CB-K21/0349
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0676
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2465
dfn-cert: DFN-CERT-2021-2422
dfn-cert: DFN-CERT-2021-2280
dfn-cert: DFN-CERT-2021-2244
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2217
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2167
dfn-cert: DFN-CERT-2021-2157
dfn-cert: DFN-CERT-2021-2156
dfn-cert: DFN-CERT-2021-2154
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2145
dfn-cert: DFN-CERT-2021-2144
dfn-cert: DFN-CERT-2021-2143
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2092
dfn-cert: DFN-CERT-2021-2071
dfn-cert: DFN-CERT-2021-2032
dfn-cert: DFN-CERT-2021-2030
dfn-cert: DFN-CERT-2021-2011
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1999
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1971
dfn-cert: DFN-CERT-2021-1955
dfn-cert: DFN-CERT-2021-1953
dfn-cert: DFN-CERT-2021-1949
dfn-cert: DFN-CERT-2021-1938
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1898
dfn-cert: DFN-CERT-2021-1897
dfn-cert: DFN-CERT-2021-1896
dfn-cert: DFN-CERT-2021-1895
dfn-cert: DFN-CERT-2021-1852
dfn-cert: DFN-CERT-2021-1842
dfn-cert: DFN-CERT-2021-1836
dfn-cert: DFN-CERT-2021-1783
dfn-cert: DFN-CERT-2021-1763
dfn-cert: DFN-CERT-2021-1761
dfn-cert: DFN-CERT-2021-1754
dfn-cert: DFN-CERT-2021-1744
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1707
dfn-cert: DFN-CERT-2021-1703
dfn-cert: DFN-CERT-2021-1699
dfn-cert: DFN-CERT-2021-1698
dfn-cert: DFN-CERT-2021-1697
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1571
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1531
dfn-cert: DFN-CERT-2021-1522
dfn-cert: DFN-CERT-2021-1426
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-0799
dfn-cert: DFN-CERT-2021-0793
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0785
dfn-cert: DFN-CERT-2021-0784

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5338-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5338-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.105.109
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. (CVE-2022-0492)
Jurgen Gross discovered that the Xen subsystem within the Linux kernel did not adequately limit the number of events driver domains (unprivileged PV backends) could send to other guest VMs. An attacker in a driver domain could use this to cause a denial of service in other guest VMs. (CVE-2021-28711, CVE-2021-28712, CVE-2021-28713)
Jurgen Gross discovered that the Xen network backend driver in the Linux kernel did not adequately limit the amount of queued packets when a guest did not process them. An attacker in a guest VM can use this to cause a denial of service (excessive kernel memory consumption) in the network backend domain. (CVE-2021-28714, CVE-2021-28715)
It was discovered that the simulated networking device driver for the Linux kernel did not properly initialize memory in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-4135)
Brendan Dolan-Gavitt discovered that the Marvell WiFi-Ex USB device driver in the Linux kernel did not properly handle some error conditions. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-43976)
It was discovered that the ARM Trusted Execution Environment (TEE) subsystem in the Linux kernel contained a race condition leading to a use- after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-44733)

. . . continues on next page . . .

... continued from previous page ...

It was discovered that the Phone Network protocol (PhoNet) implementation in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45095)
It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could possibly use this to cause a denial of service (memory exhaustion). (CVE-2021-45480)
Samuel Page discovered that the Transparent Inter-Process Communication (TIPC) protocol implementation in the Linux kernel contained a stack-based buffer overflow. A remote attacker could use this to cause a denial of service (system crash) for systems that have a TIPC bearer configured. (CVE-2022-0435)
It was discovered that the KVM implementation for s390 systems in the Linux kernel did not properly prevent memory operations on PVM guests that were in non-protected mode. A local attacker could use this to obtain unauthorized memory write access. (CVE-2022-0516)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5338-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5338.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5338-1`
`cve: CVE-2021-28711`
`cve: CVE-2021-28712`
`cve: CVE-2021-28713`
`cve: CVE-2021-28714`
`cve: CVE-2021-28715`
`cve: CVE-2021-4135`
`cve: CVE-2021-43976`
`cve: CVE-2021-44733`
`cve: CVE-2021-45095`
`cve: CVE-2021-45480`
`cve: CVE-2022-0435`
`cve: CVE-2022-0492`
`cve: CVE-2022-0516`
`advisory_id: USN-5338-1`
`cert-bund: WID-SEC-2023-0875`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2022-2062`
`cert-bund: WID-SEC-2022-0887`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0233`
`cert-bund: WID-SEC-2022-0229`
`cert-bund: WID-SEC-2022-0137`
`cert-bund: WID-SEC-2022-0061`
`cert-bund: WID-SEC-2022-0060`
`cert-bund: WID-SEC-2022-0002`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0686
cert-bund: CB-K22/0181
cert-bund: CB-K22/0176
cert-bund: CB-K22/0146
cert-bund: CB-K21/1316
cert-bund: CB-K21/1315
cert-bund: CB-K21/1306
cert-bund: CB-K21/1299
cert-bund: CB-K21/1212
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2022-1707
dfn-cert: DFN-CERT-2022-1689
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1397
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1244
dfn-cert: DFN-CERT-2022-1078
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-1037
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0895
dfn-cert: DFN-CERT-2022-0887
dfn-cert: DFN-CERT-2022-0876
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0825
dfn-cert: DFN-CERT-2022-0775
dfn-cert: DFN-CERT-2022-0765
dfn-cert: DFN-CERT-2022-0758
dfn-cert: DFN-CERT-2022-0738
dfn-cert: DFN-CERT-2022-0737
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0712
dfn-cert: DFN-CERT-2022-0711
dfn-cert: DFN-CERT-2022-0676
dfn-cert: DFN-CERT-2022-0670
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0660
dfn-cert: DFN-CERT-2022-0658
dfn-cert: DFN-CERT-2022-0657
dfn-cert: DFN-CERT-2022-0585
dfn-cert: DFN-CERT-2022-0584
dfn-cert: DFN-CERT-2022-0568

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0567
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0550
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0545
dfn-cert: DFN-CERT-2022-0544
dfn-cert: DFN-CERT-2022-0542
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0540
dfn-cert: DFN-CERT-2022-0539
dfn-cert: DFN-CERT-2022-0538
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0536
dfn-cert: DFN-CERT-2022-0535
dfn-cert: DFN-CERT-2022-0513
dfn-cert: DFN-CERT-2022-0466
dfn-cert: DFN-CERT-2022-0439
dfn-cert: DFN-CERT-2022-0433
dfn-cert: DFN-CERT-2022-0423
dfn-cert: DFN-CERT-2022-0414
dfn-cert: DFN-CERT-2022-0413
dfn-cert: DFN-CERT-2022-0372
dfn-cert: DFN-CERT-2022-0354
dfn-cert: DFN-CERT-2022-0350
dfn-cert: DFN-CERT-2022-0344
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0342
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0337
dfn-cert: DFN-CERT-2022-0336
dfn-cert: DFN-CERT-2022-0335
dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0318
dfn-cert: DFN-CERT-2022-0317
dfn-cert: DFN-CERT-2022-0251
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0193
dfn-cert: DFN-CERT-2022-0186
dfn-cert: DFN-CERT-2022-0162
dfn-cert: DFN-CERT-2022-0092
dfn-cert: DFN-CERT-2022-0090
dfn-cert: DFN-CERT-2022-0077
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2021-2653

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2466

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5415-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5415-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.110.114

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Jeremy Cline discovered a use-after-free in the nouveau graphics driver of the Linux kernel during device removal. A privileged or physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2020-27820)
Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-26401)
David Bouman discovered that the netfilter subsystem in the Linux kernel did not initialize memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-1016)
It was discovered that the MMC/SD subsystem in the Linux kernel did not properly handle read errors from SD cards in certain situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-20008)
It was discovered that the USB gadget subsystem in the Linux kernel did not properly validate interface descriptor requests. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-25258)

... continues on next page ...

... continued from previous page ...

It was discovered that the Remote NDIS (RNDIS) USB gadget implementation in the Linux kernel did not properly validate the size of the RNDIS_MSG_SET command. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-25375)
It was discovered that the ST21NFCA NFC driver in the Linux kernel did not properly validate the size of certain data in EVT_TRANSACTION events. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-26490)
It was discovered that the Xilinx USB2 device gadget driver in the Linux kernel did not properly validate endpoint indices from the host. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-27223)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5415-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5415.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5415-1`
`cve: CVE-2020-27820`
`cve: CVE-2021-26401`
`cve: CVE-2022-1016`
`cve: CVE-2022-20008`
`cve: CVE-2022-25258`
`cve: CVE-2022-25375`
`cve: CVE-2022-26490`
`cve: CVE-2022-27223`
`advisory_id: USN-5415-1`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2023-0809`
`cert-bund: WID-SEC-2022-0854`
`cert-bund: WID-SEC-2022-0853`
`cert-bund: WID-SEC-2022-0536`
`cert-bund: WID-SEC-2022-0322`
`cert-bund: WID-SEC-2022-0237`
`cert-bund: WID-SEC-2022-0227`
`cert-bund: WID-SEC-2022-0160`
`cert-bund: WID-SEC-2022-0155`
`cert-bund: WID-SEC-2022-0137`
`cert-bund: CB-K22/0686`
`cert-bund: CB-K22/0529`
`cert-bund: CB-K22/0379`
`cert-bund: CB-K22/0361`
`cert-bund: CB-K22/0309`
`cert-bund: CB-K22/0281`
`cert-bund: CB-K22/0215`
`cert-bund: CB-K22/0202`

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K21/1148
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0178
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2023-0111
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2358
dfn-cert: DFN-CERT-2022-2275
dfn-cert: DFN-CERT-2022-1853
dfn-cert: DFN-CERT-2022-1754
dfn-cert: DFN-CERT-2022-1676
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1503
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1283
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1082
dfn-cert: DFN-CERT-2022-1075
dfn-cert: DFN-CERT-2022-1074
dfn-cert: DFN-CERT-2022-1073
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-1037
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0969
dfn-cert: DFN-CERT-2022-0930
dfn-cert: DFN-CERT-2022-0921
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0915
dfn-cert: DFN-CERT-2022-0895
dfn-cert: DFN-CERT-2022-0893
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0892
dfn-cert: DFN-CERT-2022-0881
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0862
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0860
dfn-cert: DFN-CERT-2022-0840
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0803
dfn-cert: DFN-CERT-2022-0783
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0720
dfn-cert: DFN-CERT-2022-0719
dfn-cert: DFN-CERT-2022-0676
dfn-cert: DFN-CERT-2022-0663
dfn-cert: DFN-CERT-2022-0631
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0543
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0539
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0531
dfn-cert: DFN-CERT-2022-0529
dfn-cert: DFN-CERT-2022-0526
dfn-cert: DFN-CERT-2022-0513
dfn-cert: DFN-CERT-2022-0379
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0318
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0092
dfn-cert: DFN-CERT-2022-0090
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2021-2568
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5728-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi' package(s) announced via the USN-5728-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.132.132
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)
It was discovered that a race condition existed in the memory address space accounting 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-2022-41222)
It was discovered that a race condition existed in the instruction emulator of the Linux kernel on Arm 64-bit systems. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-20422)
It was discovered that the KVM implementation in the Linux kernel did not properly handle virtual CPUs without APICs in certain situations. A local attacker could possibly use this to cause a denial of service (host system crash). (CVE-2022-2153)
Hao Sun and Jiacheng Xu discovered that the NILFS file system implementation 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-2022-2978)
Johannes Wikner and Kaveh Razavi discovered that for some Intel x86-64 processors, the Linux kernel's protections against speculative branch target injection attacks were insufficient in some circumstances. A local attacker could possibly use this to expose sensitive information. (CVE-2022-29901)
Abhishek Shah discovered a race condition in the PF_KEYv2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2022-3028)

... continues on next page ...

... continued from previous page ...

It was discovered that the Netlink device interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability with some network device drivers. A local attacker with admin access to the network device could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3625)
It was discovered that the IDT 77252 ATM PCI device driver in the Linux kernel did not properly remove any pending timers during device exit, resulting in a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-3635)
Xingyuan Mo and Gengjia Chen discovered that the Promise SuperTrak EX storage controller driver in the Linux kernel did not properly handle certain structures. A local attacker could potentially use this to expose sensitive information (kernel memory). (CVE-2022-40768)
Sonke Huster discovered that a use-after-free vulnerability existed in the WiFi ... [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-5728-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5728.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5728-1`
`cve: CVE-2022-20422`
`cve: CVE-2022-2153`
`cve: CVE-2022-2978`
`cve: CVE-2022-29901`
`cve: CVE-2022-3028`
`cve: CVE-2022-3625`
`cve: CVE-2022-3635`
`cve: CVE-2022-40768`
`cve: CVE-2022-41222`
`cve: CVE-2022-42703`
`cve: CVE-2022-42719`
`advisory_id: USN-5728-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1981`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2023-1669`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0292`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2023-0018`
`cert-bund: WID-SEC-2022-1823`
`cert-bund: WID-SEC-2022-1812`
`cert-bund: WID-SEC-2022-1716`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1651
cert-bund: WID-SEC-2022-1599
cert-bund: WID-SEC-2022-1496
cert-bund: WID-SEC-2022-1454
cert-bund: WID-SEC-2022-1208
cert-bund: WID-SEC-2022-1186
cert-bund: WID-SEC-2022-0665
cert-bund: WID-SEC-2022-0659
cert-bund: WID-SEC-2022-0650
cert-bund: WID-SEC-2022-0436
dfn-cert: DFN-CERT-2024-1554
dfn-cert: DFN-CERT-2024-1059
dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2024-0371
dfn-cert: DFN-CERT-2024-0370
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1707
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1595
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1542
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1253
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-0863
dfn-cert: DFN-CERT-2023-0555
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0534
dfn-cert: DFN-CERT-2023-0508
dfn-cert: DFN-CERT-2023-0421
dfn-cert: DFN-CERT-2023-0420
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0269
dfn-cert: DFN-CERT-2023-0059
dfn-cert: DFN-CERT-2023-0021
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-2022-2899
dfn-cert: DFN-CERT-2022-2892
dfn-cert: DFN-CERT-2022-2891
dfn-cert: DFN-CERT-2022-2890
dfn-cert: DFN-CERT-2022-2879
dfn-cert: DFN-CERT-2022-2878
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2833
dfn-cert: DFN-CERT-2022-2818
dfn-cert: DFN-CERT-2022-2817
dfn-cert: DFN-CERT-2022-2787
dfn-cert: DFN-CERT-2022-2737
dfn-cert: DFN-CERT-2022-2736
dfn-cert: DFN-CERT-2022-2735
dfn-cert: DFN-CERT-2022-2733
dfn-cert: DFN-CERT-2022-2713
dfn-cert: DFN-CERT-2022-2712
dfn-cert: DFN-CERT-2022-2649
dfn-cert: DFN-CERT-2022-2646
dfn-cert: DFN-CERT-2022-2632
dfn-cert: DFN-CERT-2022-2623
dfn-cert: DFN-CERT-2022-2621
dfn-cert: DFN-CERT-2022-2620
dfn-cert: DFN-CERT-2022-2619
dfn-cert: DFN-CERT-2022-2618
dfn-cert: DFN-CERT-2022-2617
dfn-cert: DFN-CERT-2022-2616
dfn-cert: DFN-CERT-2022-2610
dfn-cert: DFN-CERT-2022-2609
dfn-cert: DFN-CERT-2022-2608
dfn-cert: DFN-CERT-2022-2599
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2544
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2469
dfn-cert: DFN-CERT-2022-2449
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2442
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2382
dfn-cert: DFN-CERT-2022-2373
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2334
dfn-cert: DFN-CERT-2022-2333
dfn-cert: DFN-CERT-2022-2326
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2298
dfn-cert: DFN-CERT-2022-2295
dfn-cert: DFN-CERT-2022-2292

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2265
dfn-cert: DFN-CERT-2022-2235
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2022-2174
dfn-cert: DFN-CERT-2022-2172
dfn-cert: DFN-CERT-2022-2171
dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2139
dfn-cert: DFN-CERT-2022-2135
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2067
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-2040
dfn-cert: DFN-CERT-2022-2038
dfn-cert: DFN-CERT-2022-2037
dfn-cert: DFN-CERT-2022-2034
dfn-cert: DFN-CERT-2022-1926
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-2022-1640
dfn-cert: DFN-CERT-2022-1598
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-2022-1557
dfn-cert: DFN-CERT-2022-1555
dfn-cert: DFN-CERT-2022-1554
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5804-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-hwe, linux-azure, linux-azure-4.15, linux-gcp, linux-gcp-5.4, linux-hwe, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5804-1 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-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.137.135
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-hwe, linux-azure, linux-azure-4.15, linux-gcp, linux-gcp-5.4, linux-hwe, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43945)
Tamas Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42896)
It was discovered that the Xen netback driver in the Linux kernel did not properly handle packets structured in certain ways. An attacker in a guest VM could possibly use this to cause a denial of service (host NIC availability). (CVE-2022-3643)
It was discovered that an integer overflow vulnerability existed in the Bluetooth subsystem in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2022-45934)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5804-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5804.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5804-1
cve: CVE-2022-3643
cve: CVE-2022-42896
cve: CVE-2022-43945
cve: CVE-2022-45934
advisory_id: USN-5804-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0794
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-2250
cert-bund: WID-SEC-2022-2176
cert-bund: WID-SEC-2022-2152
cert-bund: WID-SEC-2022-1964
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-0951
dfn-cert: DFN-CERT-2024-0700
dfn-cert: DFN-CERT-2024-0655
dfn-cert: DFN-CERT-2024-0510
dfn-cert: DFN-CERT-2023-3003
dfn-cert: DFN-CERT-2023-2479
dfn-cert: DFN-CERT-2023-2033
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-1829
dfn-cert: DFN-CERT-2023-1817
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-1094
dfn-cert: DFN-CERT-2023-1082
dfn-cert: DFN-CERT-2023-1081
dfn-cert: DFN-CERT-2023-1079
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0629
dfn-cert: DFN-CERT-2023-0611
dfn-cert: DFN-CERT-2023-0522
dfn-cert: DFN-CERT-2023-0521
dfn-cert: DFN-CERT-2023-0511
dfn-cert: DFN-CERT-2023-0485
dfn-cert: DFN-CERT-2023-0421
dfn-cert: DFN-CERT-2023-0420
dfn-cert: DFN-CERT-2023-0378
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0342
dfn-cert: DFN-CERT-2023-0333
dfn-cert: DFN-CERT-2023-0332
dfn-cert: DFN-CERT-2023-0285
dfn-cert: DFN-CERT-2023-0194
dfn-cert: DFN-CERT-2023-0185
dfn-cert: DFN-CERT-2023-0168
dfn-cert: DFN-CERT-2023-0167
dfn-cert: DFN-CERT-2023-0162

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0078
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-2022-2909
dfn-cert: DFN-CERT-2022-2905
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2894
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-2022-2881
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-2022-2876
dfn-cert: DFN-CERT-2022-2871
dfn-cert: DFN-CERT-2022-2863
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2817
dfn-cert: DFN-CERT-2022-2764
dfn-cert: DFN-CERT-2022-2733
dfn-cert: DFN-CERT-2022-2732
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5853-1)

Summary

The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gkeop, linux-kvm, linux-oracle, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5853-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
```

... continues on next page ...

... continued from previous page ...

Fixed version: >=linux-image-generic-5.4.0.139.137

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gkeop, linux-kvm, linux-oracle, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
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)
Khalid Masum discovered that the NILFS2 file system implementation in the Linux kernel did not properly handle certain error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-3649)
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)
It was discovered that the binder IPC implementation 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-2023-20928)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5853-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5853.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5853-1
cve: CVE-2022-3628
cve: CVE-2022-3640

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-3649
cve: CVE-2022-41849
cve: CVE-2022-41850
cve: CVE-2022-42895
cve: CVE-2023-20928
advisory_id: USN-5853-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-0018
cert-bund: WID-SEC-2022-2152
cert-bund: WID-SEC-2022-1903
cert-bund: WID-SEC-2022-1823
cert-bund: WID-SEC-2022-1583
dfn-cert: DFN-CERT-2024-1189
dfn-cert: DFN-CERT-2024-1037
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-0918
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0863
dfn-cert: DFN-CERT-2023-0861
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-2023-0078
dfn-cert: DFN-CERT-2023-0041
dfn-cert: DFN-CERT-2023-0021
dfn-cert: DFN-CERT-2023-0020
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-2022-2893
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

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2863
dfn-cert: DFN-CERT-2022-2737
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-2022-2550
dfn-cert: DFN-CERT-2022-2544
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2449
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-5980-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-gcp, linux-gke, linux-gkeop, linux-ibm, linux-kvm, linux-oracle, linux-raspi' package(s) announced via the USN-5980-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.146.144

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-gcp, linux-gke, linux-gkeop, linux-ibm, linux-kvm, linux-oracle, linux-raspi' package(s) on Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3669)
It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. (CVE-2022-2196)
Gerald Lee discovered that the USB Gadget file system implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-4382)
It was discovered that the RNDIS USB driver in the Linux kernel contained an integer overflow vulnerability. A local attacker with physical access could plug in a malicious USB device to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-23559)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5980-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5980.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5980-1`
`cve: CVE-2021-3669`
`cve: CVE-2022-2196`
`cve: CVE-2022-4382`
`cve: CVE-2023-23559`
`advisory_id: USN-5980-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0183`
`cert-bund: WID-SEC-2023-0045`
`cert-bund: WID-SEC-2022-2334`
`cert-bund: WID-SEC-2022-0515`
`dfn-cert: DFN-CERT-2024-0516`
`dfn-cert: DFN-CERT-2024-0513`
`dfn-cert: DFN-CERT-2024-0511`
`dfn-cert: DFN-CERT-2024-0461`
`dfn-cert: DFN-CERT-2023-2573`
`dfn-cert: DFN-CERT-2023-1955`
`dfn-cert: DFN-CERT-2023-1577`
`dfn-cert: DFN-CERT-2023-1377`
`dfn-cert: DFN-CERT-2023-1116`
`dfn-cert: DFN-CERT-2023-1081`
`dfn-cert: DFN-CERT-2023-1080`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1079
dfn-cert: DFN-CERT-2023-1076
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1002
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0996
dfn-cert: DFN-CERT-2023-0919
dfn-cert: DFN-CERT-2023-0918
dfn-cert: DFN-CERT-2023-0917
dfn-cert: DFN-CERT-2023-0906
dfn-cert: DFN-CERT-2023-0873
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0865
dfn-cert: DFN-CERT-2023-0864
dfn-cert: DFN-CERT-2023-0862
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0797
dfn-cert: DFN-CERT-2023-0739
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0632
dfn-cert: DFN-CERT-2023-0612
dfn-cert: DFN-CERT-2023-0603
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0600
dfn-cert: DFN-CERT-2023-0596
dfn-cert: DFN-CERT-2023-0592
dfn-cert: DFN-CERT-2023-0586
dfn-cert: DFN-CERT-2023-0582
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0324
dfn-cert: DFN-CERT-2023-0094
dfn-cert: DFN-CERT-2022-2113
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2120

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6340-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-hwe-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-6340-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.162.159
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-hwe-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Ruihan Li discovered that the bluetooth subsystem in the Linux kernel did not properly perform permissions checks when handling HCI sockets. A physically proximate attacker could use this to cause a denial of service (bluetooth communication). (CVE-2023-2002)
Zi Fan Tan discovered that the binder IPC implementation 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-2023-21255)
Juan Jose Lopez Jaimez, Meador Inge, Simon Scannell, and Nenad Stojanovski discovered that the BPF verifier in the Linux kernel did not properly mark registers for precision tracking in certain situations, leading to an out- of-bounds access vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-2163)
Zheng Zhang discovered that the device-mapper implementation in the Linux kernel did not properly handle locking during table_clear() operations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2269)
It was discovered that the DVB Core driver in the Linux kernel did not properly handle locking events in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-31084)
It was discovered that the kernel->user space relay implementation in the Linux kernel did not properly perform certain buffer calculations, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-3268)
It was discovered that the video4linux driver for Philips based TV cards in the Linux kernel contained a race condition during device removal, 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-2023-35823)

... continues on next page ...

... continued from previous page ...

It was discovered that the SDMC DM1105 PCI device driver in the Linux kernel contained a race condition during device removal, 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-2023-35824)
It was discovered that the Renesas USB controller driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35828)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6340-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6340.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6340-1`
`cve: CVE-2023-2002`
`cve: CVE-2023-21255`
`cve: CVE-2023-2163`
`cve: CVE-2023-2269`
`cve: CVE-2023-31084`
`cve: CVE-2023-3268`
`cve: CVE-2023-35823`
`cve: CVE-2023-35824`
`cve: CVE-2023-35828`
`advisory_id: USN-6340-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1981`
`cert-bund: WID-SEC-2023-1669`
`cert-bund: WID-SEC-2023-1612`
`cert-bund: WID-SEC-2023-1498`
`cert-bund: WID-SEC-2023-1494`
`cert-bund: WID-SEC-2023-1066`
`cert-bund: WID-SEC-2023-1062`
`cert-bund: WID-SEC-2023-0984`
`dfn-cert: DFN-CERT-2024-1087`
`dfn-cert: DFN-CERT-2024-0951`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0745`
`dfn-cert: DFN-CERT-2024-0730`
`dfn-cert: DFN-CERT-2024-0657`
`dfn-cert: DFN-CERT-2024-0656`
`dfn-cert: DFN-CERT-2024-0513`
`dfn-cert: DFN-CERT-2024-0461`
`dfn-cert: DFN-CERT-2024-0281`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0266
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0246
dfn-cert: DFN-CERT-2024-0201
dfn-cert: DFN-CERT-2024-0200
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2023-3168
dfn-cert: DFN-CERT-2023-3155
dfn-cert: DFN-CERT-2023-3145
dfn-cert: DFN-CERT-2023-3138
dfn-cert: DFN-CERT-2023-3137
dfn-cert: DFN-CERT-2023-3135
dfn-cert: DFN-CERT-2023-3133
dfn-cert: DFN-CERT-2023-3131
dfn-cert: DFN-CERT-2023-2989
dfn-cert: DFN-CERT-2023-2985
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2800
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2745
dfn-cert: DFN-CERT-2023-2744
dfn-cert: DFN-CERT-2023-2743
dfn-cert: DFN-CERT-2023-2725
dfn-cert: DFN-CERT-2023-2723
dfn-cert: DFN-CERT-2023-2721
dfn-cert: DFN-CERT-2023-2719
dfn-cert: DFN-CERT-2023-2718
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-2217
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2112
dfn-cert: DFN-CERT-2023-2075
dfn-cert: DFN-CERT-2023-2071
dfn-cert: DFN-CERT-2023-2069
dfn-cert: DFN-CERT-2023-2068
dfn-cert: DFN-CERT-2023-2067
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-2002
dfn-cert: DFN-CERT-2023-1993
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1923

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1870
dfn-cert: DFN-CERT-2023-1776
dfn-cert: DFN-CERT-2023-1753
dfn-cert: DFN-CERT-2023-1747
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1723
dfn-cert: DFN-CERT-2023-1722
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1622
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1589
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1558
dfn-cert: DFN-CERT-2023-1542
dfn-cert: DFN-CERT-2023-1541
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1528
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1447
dfn-cert: DFN-CERT-2023-1412
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1405
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1371
dfn-cert: DFN-CERT-2023-1370
dfn-cert: DFN-CERT-2023-1339
dfn-cert: DFN-CERT-2023-1100

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6167-1)

Summary
The remote host is missing an update for the 'qemu' package(s) announced via the USN-6167-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: qemu
Installed version: qemu-1:4.2-3ubuntu6.16
Fixed version: >=qemu-1:4.2-3ubuntu6.27

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

Affected Software/OS
'qemu' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that QEMU did not properly manage the guest drivers when shared buffers are not allocated. A malicious guest driver could use this issue to cause QEMU to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-1050)
It was discovered that QEMU did not properly check the size of the structure pointed to by the guest physical address pqxl. A malicious guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-4144)
It was discovered that QEMU did not properly manage memory in the ACPI Error Record Serialization Table (ERST) device. A malicious guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-4172)
It was discovered that QEMU did not properly manage memory when DMA memory writes happen repeatedly in the lsi53c895a device. A malicious guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service. (CVE-2023-0330)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6167-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6167.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6167-1
cve: CVE-2022-1050
cve: CVE-2022-4144
cve: CVE-2022-4172
cve: CVE-2023-0330
advisory_id: USN-6167-1
cert-bund: WID-SEC-2023-0649

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0173
cert-bund: WID-SEC-2022-2185
cert-bund: WID-SEC-2022-2179
cert-bund: CB-K22/0360
dfn-cert: DFN-CERT-2024-1079
dfn-cert: DFN-CERT-2023-2495
dfn-cert: DFN-CERT-2023-2424
dfn-cert: DFN-CERT-2023-2407
dfn-cert: DFN-CERT-2023-2305
dfn-cert: DFN-CERT-2023-2260
dfn-cert: DFN-CERT-2023-2236
dfn-cert: DFN-CERT-2023-1991
dfn-cert: DFN-CERT-2023-1757
dfn-cert: DFN-CERT-2023-1742
dfn-cert: DFN-CERT-2023-1402
dfn-cert: DFN-CERT-2023-1261
dfn-cert: DFN-CERT-2023-1042
dfn-cert: DFN-CERT-2023-0654
dfn-cert: DFN-CERT-2023-0626
dfn-cert: DFN-CERT-2023-0610
dfn-cert: DFN-CERT-2023-0591
dfn-cert: DFN-CERT-2023-0568
dfn-cert: DFN-CERT-2023-0526
dfn-cert: DFN-CERT-2023-0295
dfn-cert: DFN-CERT-2023-0171
dfn-cert: DFN-CERT-2023-0085
dfn-cert: DFN-CERT-2023-0022
dfn-cert: DFN-CERT-2022-2784

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6567-1)

Summary
The remote host is missing an update for the 'qemu' package(s) announced via the USN-6567-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: qemu
Installed version: qemu-1:4.2-3ubuntu6.16
Fixed version: >=qemu-1:4.2-3ubuntu6.28

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'qemu' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Gaoning Pan and Xingwei Li discovered that QEMU incorrectly handled the USB xHCI controller device. A privileged guest attacker could possibly use this issue to cause QEMU to crash, leading to a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2020-14394)
It was discovered that QEMU incorrectly handled the TCG Accelerator. A local attacker could use this issue to cause QEMU to crash, leading to a denial of service, or possibly execute arbitrary code and esclate privileges. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-24165)
It was discovered that QEMU incorrectly handled the Intel HD audio device. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2021-3611)
It was discovered that QEMU incorrectly handled the ATI VGA device. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-3638)
It was discovered that QEMU incorrectly handled the VMWare paravirtual RDMA device. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service. (CVE-2023-1544)
It was discovered that QEMU incorrectly handled the 9p passthrough filesystem. A malicious guest attacker could possibly use this issue to open special files and escape the exported 9p tree. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-2861)
It was discovered that QEMU incorrectly handled the virtual crypto device. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-3180)
It was discovered that QEMU incorrectly handled the built-in VNC server. A remote authenticated attacker could possibly use this issue to cause QEMU to stop responding, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-3255)
It was discovered that QEMU incorrectly handled net device hot-unplugging. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-3301)
It was discovered that QEMU incorrectly handled the built-in VNC server. A remote attacker could possibly use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-3354)
It was discovered that QEMU incorrectly handled NVME devices. A malicious guest attacker could use this issue to cause QEMU to crash, leading to a denial of service. This issue only affected Ubuntu 23.10. (CVE-2023-40360)
It was discovered that QEMU ... [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.

... continues on next page ...

... continued from previous page ...

Details: Ubuntu: Security Advisory (USN-6567-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6567.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6567-1
cve: CVE-2020-14394
cve: CVE-2020-24165
cve: CVE-2021-3611
cve: CVE-2021-3638
cve: CVE-2023-1544
cve: CVE-2023-2861
cve: CVE-2023-3180
cve: CVE-2023-3255
cve: CVE-2023-3301
cve: CVE-2023-3354
cve: CVE-2023-40360
cve: CVE-2023-4135
cve: CVE-2023-42467
cve: CVE-2023-5088
advisory_id: USN-6567-1
cert-bund: WID-SEC-2023-2799
cert-bund: WID-SEC-2023-2302
cert-bund: WID-SEC-2023-2197
cert-bund: WID-SEC-2023-2059
cert-bund: WID-SEC-2023-1965
cert-bund: WID-SEC-2023-1963
cert-bund: WID-SEC-2023-1960
cert-bund: WID-SEC-2023-1755
cert-bund: WID-SEC-2023-1709
cert-bund: WID-SEC-2023-1662
cert-bund: WID-SEC-2023-1621
cert-bund: WID-SEC-2022-2259
cert-bund: WID-SEC-2022-2257
cert-bund: WID-SEC-2022-1115
cert-bund: CB-K22/0263
cert-bund: CB-K21/0677
cert-bund: CB-K21/0021
dfn-cert: DFN-CERT-2024-1388
dfn-cert: DFN-CERT-2024-1142
dfn-cert: DFN-CERT-2024-1079
dfn-cert: DFN-CERT-2024-0959
dfn-cert: DFN-CERT-2024-0911
dfn-cert: DFN-CERT-2024-0652
dfn-cert: DFN-CERT-2024-0234
dfn-cert: DFN-CERT-2024-0040
dfn-cert: DFN-CERT-2023-3065

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-2869
dfn-cert: DFN-CERT-2023-2495
dfn-cert: DFN-CERT-2023-2424
dfn-cert: DFN-CERT-2023-2407
dfn-cert: DFN-CERT-2023-2305
dfn-cert: DFN-CERT-2023-2260
dfn-cert: DFN-CERT-2023-2236
dfn-cert: DFN-CERT-2023-2215
dfn-cert: DFN-CERT-2023-2135
dfn-cert: DFN-CERT-2023-1991
dfn-cert: DFN-CERT-2023-1982
dfn-cert: DFN-CERT-2023-1840
dfn-cert: DFN-CERT-2023-1757
dfn-cert: DFN-CERT-2023-1742
dfn-cert: DFN-CERT-2023-1138
dfn-cert: DFN-CERT-2023-0655
dfn-cert: DFN-CERT-2023-0626
dfn-cert: DFN-CERT-2023-0591
dfn-cert: DFN-CERT-2023-0568
dfn-cert: DFN-CERT-2023-0295
dfn-cert: DFN-CERT-2023-0171
dfn-cert: DFN-CERT-2023-0022
dfn-cert: DFN-CERT-2022-2784
dfn-cert: DFN-CERT-2022-2570
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2065
dfn-cert: DFN-CERT-2021-1824
dfn-cert: DFN-CERT-2021-1637
dfn-cert: DFN-CERT-2021-1585
dfn-cert: DFN-CERT-2021-1572
dfn-cert: DFN-CERT-2021-1567
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5142-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5142-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.14+dfsg-0ubuntu0.20.04.1
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Stefan Metzmacher discovered that Samba incorrectly handled SMB1 client connections. A remote attacker could possibly use this issue to downgrade connections to plaintext authentication. (CVE-2016-2124)
Andrew Bartlett discovered that Samba incorrectly mapping domain users to local users. An authenticated attacker could possibly use this issue to become root on domain members. (CVE-2020-25717)
Andrew Bartlett discovered that Samba did not correctly sandbox Kerberos tickets issues by an RODC. An RODC could print administrator tickets, contrary to expectations. (CVE-2020-25718)
Andrew Bartlett discovered that Samba incorrectly handled Kerberos tickets. Delegated administrators could possibly use this issue to impersonate accounts, leading to total domain compromise. (CVE-2020-25719)
Andrew Bartlett discovered that Samba did not provide stable AD identifiers to Kerberos acceptors. (CVE-2020-25721)
Andrew Bartlett discovered that Samba did not properly check sensitive attributes. An authenticated attacker could possibly use this issue to escalate privileges. (CVE-2020-25722)
Stefan Metzmacher discovered that Samba incorrectly handled certain large DCE/RPC requests. A remote attacker could possibly use this issue to bypass signature requirements. (CVE-2021-23192)
William Ross discovered that Samba incorrectly handled memory. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly escalate privileges. (CVE-2021-3738)
Joseph Sutton discovered that Samba incorrectly handled certain TGS requests. An authenticated attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2021-3671)
The fix for CVE-2020-25717 results in possible behaviour changes that could affect certain envi-link moved to refer
ronments. Please see the upstream advisory for more information:link moved to references>

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5142-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5142.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5142-1`
`url: https://www.samba.org/samba/security/CVE-2020-25717.html`

... continues on next page ...

... continued from previous page ...

cve: CVE-2016-2124
cve: CVE-2020-25717
cve: CVE-2020-25718
cve: CVE-2020-25719
cve: CVE-2020-25721
cve: CVE-2020-25722
cve: CVE-2021-23192
cve: CVE-2021-3671
cve: CVE-2021-3738
advisory_id: USN-5142-1
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2279
cert-bund: WID-SEC-2022-1714
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1173
cert-bund: CB-K21/1034
dfn-cert: DFN-CERT-2023-2166
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2269
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0348
dfn-cert: DFN-CERT-2022-0332
dfn-cert: DFN-CERT-2022-0293
dfn-cert: DFN-CERT-2021-2625
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2539
dfn-cert: DFN-CERT-2021-2488
dfn-cert: DFN-CERT-2021-2424
dfn-cert: DFN-CERT-2021-2412
dfn-cert: DFN-CERT-2021-2330

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5142-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5142-2 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.14+dfsg-0ubuntu0.20.04.3
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
USN-5142-1 fixed vulnerabilities in Samba. Some of the upstream changes introduced regressions in name mapping and backups.
Please see the following upstream bugs for more information: [link moved to references] [link moved to references]
This update fixes the problem.
Original advisory details:
Stefan Metzmacher discovered that Samba incorrectly handled SMB1 client connections. A remote attacker could possibly use this issue to downgrade connections to plaintext authentication. (CVE-2016-2124)
Andrew Bartlett discovered that Samba incorrectly mapping domain users to local users. An authenticated attacker could possibly use this issue to become root on domain members. (CVE-2020-25717)
Andrew Bartlett discovered that Samba did not correctly sandbox Kerberos tickets issues by an RODC. An RODC could print administrator tickets, contrary to expectations. (CVE-2020-25718)
Andrew Bartlett discovered that Samba incorrectly handled Kerberos tickets. Delegated administrators could possibly use this issue to impersonate accounts, leading to total domain compromise. (CVE-2020-25719)
Andrew Bartlett discovered that Samba did not provide stable AD identifiers to Kerberos acceptors. (CVE-2020-25721)
Andrew Bartlett discovered that Samba did not properly check sensitive attributes. An authenticated attacker could possibly use this issue to escalate privileges. (CVE-2020-25722)
Stefan Metzmacher discovered that Samba incorrectly handled certain large DCE/RPC requests. A remote attacker could possibly use this issue to bypass signature requirements. (CVE-2021-23192)
William Ross discovered that Samba incorrectly handled memory. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly escalate privileges. (CVE-2021-3738)
Joseph Sutton discovered that Samba incorrectly handled certain TGS requests. An authenticated attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2021-3671)

... continues on next page ...

... continued from previous page ...

The fix for CVE-2020-25717 results in possible behaviour changes that could affect certain envi-link moved to refer ronments. Please see the upstream advisory for more information:link moved to references>

Vulnerability Detection Method

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

Details: Ubuntu: Security Advisory (USN-5142-2)

OID:1.3.6.1.4.1.25623.1.1.12.2021.5142.2

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5142-2
url: https://bugzilla.samba.org/show_bug.cgi?id=14901
url: https://bugzilla.samba.org/show_bug.cgi?id=14918
url: https://www.samba.org/samba/security/CVE-2020-25717.html
url: https://launchpad.net/bugs/1950363
url: https://launchpad.net/bugs/1952187
cve: CVE-2016-2124
cve: CVE-2020-25717
cve: CVE-2020-25718
cve: CVE-2020-25719
cve: CVE-2020-25721
cve: CVE-2020-25722
cve: CVE-2021-23192
cve: CVE-2021-3671
cve: CVE-2021-3738
advisory_id: USN-5142-2
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2279
cert-bund: WID-SEC-2022-1714
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1173
cert-bund: CB-K21/1034
dfn-cert: DFN-CERT-2023-2166
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2269
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0348
dfn-cert: DFN-CERT-2022-0332

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0293
dfn-cert: DFN-CERT-2021-2625
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2539
dfn-cert: DFN-CERT-2021-2488
dfn-cert: DFN-CERT-2021-2424
dfn-cert: DFN-CERT-2021-2412
dfn-cert: DFN-CERT-2021-2330
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5142-3)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5142-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.14+dfsg-0ubuntu0.20.04.4
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
USN-5142-1 fixed vulnerabilities in Samba. Some of the upstream changes introduced a regression in Kerberos authentication in certain environments.
Please see the following upstream bug for more information: [link moved to references]
This update fixes the problem.
Original advisory details:
Stefan Metzmacher discovered that Samba incorrectly handled SMB1 client connections. A remote attacker could possibly use this issue to downgrade connections to plaintext authentication. (CVE-2016-2124)
Andrew Bartlett discovered that Samba incorrectly mapping domain users to local users. An authenticated attacker could possibly use this issue to become root on domain members. (CVE-2020-25717)
Andrew Bartlett discovered that Samba did not correctly sandbox Kerberos tickets issues by an RODC. An RODC could print administrator tickets, contrary to expectations. (CVE-2020-25718)

... continues on next page ...

... continued from previous page ...

Andrew Bartlett discovered that Samba incorrectly handled Kerberos tickets. Delegated administrators could possibly use this issue to impersonate accounts, leading to total domain compromise. (CVE-2020-25719)
Andrew Bartlett discovered that Samba did not provide stable AD identifiers to Kerberos acceptors. (CVE-2020-25721)
Andrew Bartlett discovered that Samba did not properly check sensitive attributes. An authenticated attacker could possibly use this issue to escalate privileges. (CVE-2020-25722)
Stefan Metzmacher discovered that Samba incorrectly handled certain large DCE/RPC requests. A remote attacker could possibly use this issue to bypass signature requirements. (CVE-2021-23192)
William Ross discovered that Samba incorrectly handled memory. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly escalate privileges. (CVE-2021-3738)
Joseph Sutton discovered that Samba incorrectly handled certain TGS requests. An authenticated attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2021-3671)
The fix for CVE-2020-25717 results in possible behaviour changes that could affect certain envi-link moved to refer
ronments. Please see the upstream advisory for more information:link moved to references>

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5142-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5142.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5142-3`
`url: https://bugzilla.samba.org/show_bug.cgi?id=14922`
`url: https://www.samba.org/samba/security/CVE-2020-25717.html`
`url: https://launchpad.net/bugs/1950363`
`cve: CVE-2016-2124`
`cve: CVE-2020-25717`
`cve: CVE-2020-25718`
`cve: CVE-2020-25719`
`cve: CVE-2020-25721`
`cve: CVE-2020-25722`
`cve: CVE-2021-23192`
`cve: CVE-2021-3671`
`cve: CVE-2021-3738`
`advisory_id: USN-5142-3`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-2279`
`cert-bund: WID-SEC-2022-1714`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0676`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1173
cert-bund: CB-K21/1034
dfn-cert: DFN-CERT-2023-2166
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2269
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0348
dfn-cert: DFN-CERT-2022-0332
dfn-cert: DFN-CERT-2022-0293
dfn-cert: DFN-CERT-2021-2625
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2539
dfn-cert: DFN-CERT-2021-2488
dfn-cert: DFN-CERT-2021-2424
dfn-cert: DFN-CERT-2021-2412
dfn-cert: DFN-CERT-2021-2330
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5260-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5260-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:    samba
Installed version:     samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.17~dfsg-0ubuntu0.21.04.1
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Orange Tsai discovered that the Samba vfs_fruit module incorrectly handled certain memory operations. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code as root. (CVE-2021-44142)
Michael Hanselmann discovered that Samba incorrectly created directories. In certain configurations, a remote attacker could possibly create a directory on the server outside of the shared directory. (CVE-2021-43566)
Kees van Vloten discovered that Samba incorrectly handled certain aliased SPN checks. A remote attacker could possibly use this issue to impersonate services. (CVE-2022-0336)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5260-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5260.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5260-1`
`cve: CVE-2021-43566`
`cve: CVE-2021-44142`
`cve: CVE-2022-0336`
`advisory_id: USN-5260-1`
`cert-bund: WID-SEC-2023-2979`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0466`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K22/0128`
`cert-bund: CB-K22/0016`
`dfn-cert: DFN-CERT-2022-0865`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0348`
`dfn-cert: DFN-CERT-2022-0332`
`dfn-cert: DFN-CERT-2022-0264`
`dfn-cert: DFN-CERT-2022-0242`
`dfn-cert: DFN-CERT-2022-0239`
`dfn-cert: DFN-CERT-2022-0232`
`dfn-cert: DFN-CERT-2022-0228`
`dfn-cert: DFN-CERT-2022-0035`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5542-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5542-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.13.17~dfsg-0ubuntu1.20.04.1
```

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

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

Vulnerability Insight
It was discovered that Samba did not handle MaxQueryDuration when being used in AD DC configurations, contrary to expectations. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-3670)
Luke Howard discovered that Samba incorrectly handled certain restrictions associated with changing passwords. A remote attacker being requested to change passwords could possibly use this issue to escalate privileges. (CVE-2022-2031)
Luca Moro discovered that Samba incorrectly handled certain SMB1 communications. A remote attacker could possibly use this issue to obtain sensitive memory contents. (CVE-2022-32742)
Joseph Sutton discovered that Samba incorrectly handled certain password change requests. A remote attacker could use this issue to change passwords of other users, resulting in privilege escalation. (CVE-2022-32744)
Joseph Sutton discovered that Samba incorrectly handled certain LDAP add or modify requests. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-32745)
Joseph Sutton and Andrew Bartlett discovered that Samba incorrectly handled certain LDAP add or modify requests. A remote attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-32746)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5542-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5542.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5542-1
cve: CVE-2021-3670
cve: CVE-2022-2031
cve: CVE-2022-32742
cve: CVE-2022-32744
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-32745
cve: CVE-2022-32746
advisory_id: USN-5542-1
cert-bund: WID-SEC-2022-0842
cert-bund: WID-SEC-2022-0588
cert-bund: CB-K22/0490
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2023-0713
dfn-cert: DFN-CERT-2023-0199
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2023-0089
dfn-cert: DFN-CERT-2022-2804
dfn-cert: DFN-CERT-2022-2514
dfn-cert: DFN-CERT-2022-1686
dfn-cert: DFN-CERT-2022-1674
dfn-cert: DFN-CERT-2022-1662
dfn-cert: DFN-CERT-2022-1025

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5292-1)

Summary
The remote host is missing an update for the 'snapd' package(s) announced via the USN-5292-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: snapd
Installed version: snapd-2.49.2+20.04
Fixed version: >=snapd-2.54.3+20.04

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

Affected Software/OS
'snapd' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. (CVE-2021-3155)

... continues on next page ...

... continued from previous page ...

Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. (CVE-2021-4120)
The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. (CVE-2021-44730)
The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code. (CVE-2021-44731)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5292-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5292.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5292-1`
`cve: CVE-2021-3155`
`cve: CVE-2021-4120`
`cve: CVE-2021-44730`
`cve: CVE-2021-44731`
`advisory_id: USN-5292-1`
`cert-bund: CB-K22/0212`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0406`
`dfn-cert: DFN-CERT-2022-0387`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5292-4)

Summary
The remote host is missing an update for the 'snapd' package(s) announced via the USN-5292-4 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:    snapd
Installed version:     snapd-2.49.2+20.04
Fixed version:      >=snapd-2.54.3+20.04.1ubuntu0.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'snapd' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
USN-5292-1 fixed a vulnerability in snapd. Unfortunately that update introduced a regression that could break the fish shell. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. (CVE-2021-3155)
Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. (CVE-2021-4120)
The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. (CVE-2021-44730)
The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code. (CVE-2021-44731)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5292-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5292.4
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5292-4`
`url: https://bugs.launchpad.net/ubuntu/+source/snapd/+bug/1961365`
`url: https://bugs.launchpad.net/ubuntu/+source/snapd/+bug/1961791`
`cve: CVE-2021-3155`
`cve: CVE-2021-4120`
`cve: CVE-2021-44730`
`cve: CVE-2021-44731`
`advisory_id: USN-5292-4`
`cert-bund: CB-K22/0212`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0406`
`dfn-cert: DFN-CERT-2022-0387`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5058-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5058-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:78.13.0+build1-0ubuntu0.20.04.2
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Thunderbird didn't ignore IMAP server responses prior to completion of the STARTTLS handshake. A person-in-the-middle could potentially exploit this to trick Thunderbird into showing incorrect information. (CVE-2021-29969)
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, or execute arbitrary code. (CVE-2021-29970, CVE-2021-29976, CVE-2021-29980, CVE-2021-29984, CVE-2021-29985, CVE-2021-29986, CVE-2021-29988, CVE-2021-29989, CVE-2021-30547)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5058-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5058.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5058-1
cve: CVE-2021-29969
cve: CVE-2021-29970
cve: CVE-2021-29976
cve: CVE-2021-29980
cve: CVE-2021-29984
cve: CVE-2021-29985
cve: CVE-2021-29986
cve: CVE-2021-29988
cve: CVE-2021-29989
cve: CVE-2021-30547
advisory_id: USN-5058-1
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1112
cert-bund: WID-SEC-2022-1022
cert-bund: CB-K21/0861
cert-bund: CB-K21/0753
cert-bund: CB-K21/0645
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1732
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1700
dfn-cert: DFN-CERT-2021-1695
dfn-cert: DFN-CERT-2021-1492
dfn-cert: DFN-CERT-2021-1481
dfn-cert: DFN-CERT-2021-1479
dfn-cert: DFN-CERT-2021-1259

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5146-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5146-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:78.14.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, or execute arbitrary code.

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-5146-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5146.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5146-1
cve: CVE-2021-38493
advisory_id: USN-5146-1
cert-bund: WID-SEC-2022-1024
cert-bund: CB-K21/0939
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-1889
dfn-cert: DFN-CERT-2021-1888
dfn-cert: DFN-CERT-2021-1871

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5393-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5393-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:91.8.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, conduct spoofing attacks, or execute arbitrary code. (CVE-2022-1097, CVE-2022-1196, CVE-2022-28281, CVE-2022-28282, CVE-2022-28285, CVE-2022-28286, CVE-2022-28289)

... continues on next page ...

... continued from previous page ...

It was discovered that Thunderbird ignored OpenPGP revocation when importing a revoked key in some circumstances. An attacker could potentially exploit this by tricking the user into trusting the authenticity of a message or tricking them into use a revoked key to send an encrypted message. (CVE-2022-1197)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5393-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5393.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5393-1`
`cve: CVE-2022-1097`
`cve: CVE-2022-1196`
`cve: CVE-2022-1197`
`cve: CVE-2022-28281`
`cve: CVE-2022-28282`
`cve: CVE-2022-28285`
`cve: CVE-2022-28286`
`cve: CVE-2022-28289`
`advisory_id: USN-5393-1`
`cert-bund: WID-SEC-2023-0838`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0482`
`cert-bund: CB-K22/0396`
`dfn-cert: DFN-CERT-2022-1430`
`dfn-cert: DFN-CERT-2022-0991`
`dfn-cert: DFN-CERT-2022-0769`
`dfn-cert: DFN-CERT-2022-0763`
`dfn-cert: DFN-CERT-2022-0762`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5663-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5663-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.2.2+build1-0ubuntu0.20.04.1
```

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, spoof the mouse pointer position, obtain sensitive information, spoof the contents of the addressbar, bypass security restrictions, or execute arbitrary code. (CVE-2022-2505, CVE-2022-36318, CVE-2022-36319, CVE-2022-38472, CVE-2022-38473, CVE-2022-38476 CVE-2022-38477, CVE-2022-38478)
Multiple security issues were discovered in Thunderbird. An attacker could potentially exploit these in order to determine when a user opens a specially crafted message. (CVE-2022-3032, CVE-2022-3034)
It was discovered that Thunderbird did not correctly handle HTML messages that contain a meta tag in some circumstances. If a user were tricked into replying to a specially crafted message, an attacker could potentially exploit this to obtain sensitive information. (CVE-2022-3033)
A security issue was discovered with the Matrix SDK in Thunderbird. An attacker sharing a room with a user could potentially exploit this to cause a denial of service. (CVE-2022-36059)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5663-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5663.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5663-1`
`cve: CVE-2022-2505`
`cve: CVE-2022-3032`
`cve: CVE-2022-3033`
`cve: CVE-2022-3034`
`cve: CVE-2022-36059`
`cve: CVE-2022-36318`
`cve: CVE-2022-36319`
`cve: CVE-2022-38472`
`cve: CVE-2022-38473`
`cve: CVE-2022-38476`
`cve: CVE-2022-38477`
`cve: CVE-2022-38478`
`advisory_id: USN-5663-1`
`cert-bund: WID-SEC-2023-0561`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1246
cert-bund: WID-SEC-2022-1167
cert-bund: WID-SEC-2022-0859
cert-bund: WID-SEC-2022-0837
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2225
dfn-cert: DFN-CERT-2022-2179
dfn-cert: DFN-CERT-2022-2056
dfn-cert: DFN-CERT-2022-1917
dfn-cert: DFN-CERT-2022-1865
dfn-cert: DFN-CERT-2022-1864
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1679
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1654

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5724-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5724-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:102.4.2+build2-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, bypass Content Security Policy (CSP) or other security restrictions, or execute arbitrary code. These issues only affect Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3266, CVE-2022-40956, CVE-2022-40957, CVE-2022-40958, CVE-2022-40959, CVE-2022-40960, CVE-2022-40962)

... continues on next page ...

... continued from previous page ...

Multiple security issues were discovered in the Matrix SDK bundled with Thunderbird. An attacker could potentially exploit these in order to impersonate another user. These issues only affect Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-39236, CVE-2022-39249, CVE-2022-39250, CVE-2022-39251)
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. (CVE-2022-42927, CVE-2022-42928, CVE-2022-42929, CVE-2022-42932)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5724-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5724.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5724-1`
`cve: CVE-2022-3266`
`cve: CVE-2022-39236`
`cve: CVE-2022-39249`
`cve: CVE-2022-39250`
`cve: CVE-2022-39251`
`cve: CVE-2022-40956`
`cve: CVE-2022-40957`
`cve: CVE-2022-40958`
`cve: CVE-2022-40959`
`cve: CVE-2022-40960`
`cve: CVE-2022-40962`
`cve: CVE-2022-42927`
`cve: CVE-2022-42928`
`cve: CVE-2022-42929`
`cve: CVE-2022-42932`
`advisory_id: USN-5724-1`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-1791`
`cert-bund: WID-SEC-2022-1589`
`cert-bund: WID-SEC-2022-1497`
`cert-bund: WID-SEC-2022-1484`
`dfn-cert: DFN-CERT-2022-2601`
`dfn-cert: DFN-CERT-2022-2551`
`dfn-cert: DFN-CERT-2022-2369`
`dfn-cert: DFN-CERT-2022-2301`
`dfn-cert: DFN-CERT-2022-2161`
`dfn-cert: DFN-CERT-2022-2104`
`dfn-cert: DFN-CERT-2022-2090`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5943-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5943-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.8.0+build2-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-0616, CVE-2023-25735, CVE-2023-25737, CVE-2023-25739, CVE-2023-25729, CVE-2023-25742, CVE-2023-25746)
Johan Carlsson discovered that Thunderbird did not properly implement CSP policy on a header when using iframes. An attacker could potentially exploits this to exfiltrate data. (CVE-2023-25728)
Irvan Kurniawan discovered that Thunderbird was not properly handling background fullscreen scripts when the window goes into fullscreen mode. An attacker could possibly use this issue to spoof the user and obtain sensitive information. (CVE-2023-25730)
Christian Holler discovered that Thunderbird did not properly check the Safe Bag attributes in PKCS 12 certificate bundle. An attacker could possibly use this issue to write to arbitrary memory by sending malicious PKCS 12 certificate. (CVE-2023-0767)
Ronald Crane discovered that Thunderbird did not properly check the size of the input being encoded in xpcom. An attacker could possibly use this issue to perform out of bound memory write operations. (CVE-2023-25732)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5943-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5943.1
Version used: `2024-02-02T04:09:01Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5943-1
cve: CVE-2023-0616
cve: CVE-2023-0767
cve: CVE-2023-25728
cve: CVE-2023-25729
cve: CVE-2023-25730
cve: CVE-2023-25732
cve: CVE-2023-25735
cve: CVE-2023-25737
cve: CVE-2023-25739
cve: CVE-2023-25742
cve: CVE-2023-25746
advisory_id: USN-5943-1
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0407
cert-bund: WID-SEC-2023-0385
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0843
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
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5972-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-5972-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.9.0+build1-0ubuntu0.20.04.1
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-25152, CVE-2023-28162, CVE-2023-28176)
Lukas Bernhard discovered that Thunderbird did not properly manage memory when invalidating JIT code while following an iterator. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-25751)
Luan Herrera discovered that Thunderbird did not properly manage cross-origin iframe when dragging a URL. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-28164)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5972-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5972.1
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-5972-1`
`cve: CVE-2023-25751`
`cve: CVE-2023-25752`
`cve: CVE-2023-28162`
`cve: CVE-2023-28164`
`cve: CVE-2023-28176`
`advisory_id: USN-5972-1`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0673`
`cert-bund: WID-SEC-2023-0643`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0741`
`dfn-cert: DFN-CERT-2023-0738`
`dfn-cert: DFN-CERT-2023-0579`
`dfn-cert: DFN-CERT-2023-0557`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6015-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6015-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:102.10.0+build2-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-1945, CVE-2023-29548, CVE-2023-29550)
Paul Menzel discovered that Thunderbird did not properly validate OCSP revocation status of recipient certificates when sending S/Mime encrypted email. An attacker could potentially exploits this issue to perform spoofing attack. (CVE-2023-0547)
Ribose RNP Team discovered that Thunderbird did not properly manage memory when parsing certain OpenPGP messages. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29479)
Irvan Kurniawan discovered that Thunderbird did not properly manage fullscreen notifications using a combination of window.open, fullscreen requests, window.name assignments, and setInterval calls. An attacker could potentially exploit this issue to perform spoofing attacks. (CVE-2023-29533)
Lukas Bernhard discovered that Thunderbird did not properly manage memory when doing Garbage Collector compaction. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29535)
Zx from qriousec discovered that Thunderbird did not properly validate the address to free a pointer provided to the memory manager. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-29536)
Trung Pham discovered that Thunderbird did not properly validate the filename directive in the Content-Disposition header. An attacker could possibly exploit this to perform reflected file download attacks potentially tricking users to install malware. (CVE-2023-29539)
Ameen Basha M K discovered that Thunderbird did not properly validate downloads of files ending in .desktop. An attacker could potentially exploits this issue to execute arbitrary code. (CVE-2023-29541)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6015-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6015.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-6015-1
cve: CVE-2023-0547
cve: CVE-2023-1945
cve: CVE-2023-29479
cve: CVE-2023-29533
cve: CVE-2023-29535
cve: CVE-2023-29536
cve: CVE-2023-29539
cve: CVE-2023-29541
cve: CVE-2023-29548
cve: CVE-2023-29550
advisory_id: USN-6015-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0941
dfn-cert: DFN-CERT-2023-1243
dfn-cert: DFN-CERT-2023-0937
dfn-cert: DFN-CERT-2023-0838
dfn-cert: DFN-CERT-2023-0805
dfn-cert: DFN-CERT-2023-0804

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6075-1)

Summary

The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6075-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:102.11.0+build1-0ubuntu0.20.04.1

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'thunderbird' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-32205, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215)
Irvan Kurniawan discovered that Thunderbird did not properly manage memory when using RLBox Expat driver. An attacker could potentially exploits this issue to cause a denial of service. (CVE-2023-32206)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6075-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6075.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6075-1`
`cve: CVE-2023-32205`
`cve: CVE-2023-32206`
`cve: CVE-2023-32207`
`cve: CVE-2023-32211`
`cve: CVE-2023-32212`
`cve: CVE-2023-32213`
`cve: CVE-2023-32215`
`advisory_id: USN-6075-1`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1201`
`cert-bund: WID-SEC-2023-1172`
`dfn-cert: DFN-CERT-2023-1751`
`dfn-cert: DFN-CERT-2023-1243`
`dfn-cert: DFN-CERT-2023-1090`
`dfn-cert: DFN-CERT-2023-1040`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6368-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6368-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  thunderbird`
`Installed version:  thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2`

... continues on next page ...

... continued from previous page ...

Fixed version: >=thunderbird-1:102.15.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-4573, CVE-2023-4574, CVE-2023-4575, CVE-2023-4581, CVE-2023-4584)
It was discovered that Thunderbird did not properly manage memory when handling WebP images. If a user were tricked into opening a malicious WebP image file, an attacker could potentially exploit these to cause a denial of service or execute arbitrary code. (CVE-2023-4863)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6368-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6368.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6368-1
cve: CVE-2023-4573
cve: CVE-2023-4574
cve: CVE-2023-4575
cve: CVE-2023-4581
cve: CVE-2023-4584
cve: CVE-2023-4863
advisory_id: USN-6368-1
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-3099
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2841
cert-bund: WID-SEC-2023-2548
cert-bund: WID-SEC-2023-2538
cert-bund: WID-SEC-2023-2313
cert-bund: WID-SEC-2023-2310
cert-bund: WID-SEC-2023-2305
cert-bund: WID-SEC-2023-2202
dfn-cert: DFN-CERT-2024-0174

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2542
dfn-cert: DFN-CERT-2023-2356
dfn-cert: DFN-CERT-2023-2325
dfn-cert: DFN-CERT-2023-2303
dfn-cert: DFN-CERT-2023-2283
dfn-cert: DFN-CERT-2023-2282
dfn-cert: DFN-CERT-2023-2190
dfn-cert: DFN-CERT-2023-2176
dfn-cert: DFN-CERT-2023-2152
dfn-cert: DFN-CERT-2023-2149
dfn-cert: DFN-CERT-2023-2120
dfn-cert: DFN-CERT-2023-2119
dfn-cert: DFN-CERT-2023-2110
dfn-cert: DFN-CERT-2023-2028
dfn-cert: DFN-CERT-2023-2004

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6515-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6515-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:115.5.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2023-6206, CVE-2023-6212)

... continues on next page ...

... continued from previous page ...

It was discovered that Thudnerbird did not properly manage memory when images were created on the canvas element. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6204)
It discovered that Thunderbird incorrectly handled certain memory when using a MessagePort. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6205)
It discovered that Thunderbird incorrectly did not properly manage ownership in ReadableByteStreams. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6207)
It discovered that Thudnerbird incorrectly did not properly manage copy operations when using Selection API in X11. An attacker could potentially exploit this issue to obtain sensitive information. (CVE-2023-6208)
Rachmat Abdul Rokhim discovered that Thunderbird incorrectly handled parsing of relative URLS starting with '///'. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2023-6209)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6515-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6515.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6515-1`
`cve: CVE-2023-6204`
`cve: CVE-2023-6205`
`cve: CVE-2023-6206`
`cve: CVE-2023-6207`
`cve: CVE-2023-6208`
`cve: CVE-2023-6209`
`cve: CVE-2023-6212`
`advisory_id: USN-6515-1`
`cert-bund: WID-SEC-2023-2995`
`dfn-cert: DFN-CERT-2024-0174`
`dfn-cert: DFN-CERT-2023-3078`
`dfn-cert: DFN-CERT-2023-2922`
`dfn-cert: DFN-CERT-2023-2920`

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6563-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6563-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:115.6.0+build2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'thunderbird' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code.(CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6861, CVE-2023-6862, CVE-2023-6863, CVE-2023-6864)
Marcus Brinkmann discovered that Thunderbird did not properly parse a PGP/MIME payload that contains digitally signed text. An attacker could potentially exploit this issue to spoof an email message. (CVE-2023-50762)
Marcus Brinkmann discovered that Thunderbird did not properly compare the signature creation date with the message date and time when using digitally signed S/MIME email message. An attacker could potentially exploit this issue to spoof date and time of an email message. (CVE-2023-50761)
DoHyun Lee discovered that Thunderbird did not properly manage memory when used on systems with the Mesa VM driver. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2023-6856)
Andrew Osmond discovered that Thunderbird did not properly validate the textures produced by remote decoders. An attacker could potentially exploit this issue to escape the sandbox. (CVE-2023-6860)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6563-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6563.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6563-1
cve: CVE-2023-50761
cve: CVE-2023-50762
cve: CVE-2023-6856
cve: CVE-2023-6857
cve: CVE-2023-6858
cve: CVE-2023-6859
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-6860
cve: CVE-2023-6861
cve: CVE-2023-6862
cve: CVE-2023-6863
cve: CVE-2023-6864
advisory_id: USN-6563-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-3185
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0168
dfn-cert: DFN-CERT-2023-3181
dfn-cert: DFN-CERT-2023-3180

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-6669-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6669-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:115.8.1+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-0741, CVE-2024-0742, CVE-2024-0747, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0755, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1936)
Cornel Ionce discovered that Thunderbird did not properly manage memory when opening the print preview dialog. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-0746)

... continues on next page ...

... continued from previous page ...

Alfred Peters discovered that Thunderbird did not properly manage memory when storing and re-accessing data on a networking channel. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1546)
Johan Carlsson discovered that Thunderbird incorrectly handled Set-Cookie response headers in multipart HTTP responses. An attacker could potentially exploit this issue to inject arbitrary cookie values. (CVE-2024-1551)
Gary Kwong discovered that Thunderbird incorrectly generated codes on 32-bit ARM devices, which could lead to unexpected numeric conversions or undefined behaviour. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-1552)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6669-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6669.1
Version used: `2024-03-06T08:59:21Z`

References
`url: https://ubuntu.com/security/notices/USN-6669-1`
`cve: CVE-2024-0741`
`cve: CVE-2024-0742`
`cve: CVE-2024-0746`
`cve: CVE-2024-0747`
`cve: CVE-2024-0749`
`cve: CVE-2024-0750`
`cve: CVE-2024-0751`
`cve: CVE-2024-0753`
`cve: CVE-2024-0755`
`cve: CVE-2024-1546`
`cve: CVE-2024-1547`
`cve: CVE-2024-1548`
`cve: CVE-2024-1549`
`cve: CVE-2024-1550`
`cve: CVE-2024-1551`
`cve: CVE-2024-1552`
`cve: CVE-2024-1553`
`cve: CVE-2024-1936`
`advisory_id: USN-6669-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0545`
`cert-bund: WID-SEC-2024-0443`
`cert-bund: WID-SEC-2024-0185`
`dfn-cert: DFN-CERT-2024-0815`
`dfn-cert: DFN-CERT-2024-0795`
`dfn-cert: DFN-CERT-2024-0784`
`dfn-cert: DFN-CERT-2024-0569`
`dfn-cert: DFN-CERT-2024-0562`
`dfn-cert: DFN-CERT-2024-0455`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0449
dfn-cert: DFN-CERT-2024-0188
dfn-cert: DFN-CERT-2024-0187

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5740-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-16.04, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5740-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: xserver-xorg-core
Installed version: xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.4
Vulnerable package: xwayland
Installed version: xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xwayland-2:1.20.13-1ubuntu1~20.04.4

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

Affected Software/OS
'xorg-server, xorg-server-hwe-16.04, xorg-server-hwe-18.04, xwayland' 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 X.Org X Server incorrectly handled certain inputs. An attacker could use these issues to cause the server to crash, resulting in 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-5740-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5740.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5740-1
cve: CVE-2022-3550
cve: CVE-2022-3551
advisory_id: USN-5740-1

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1759
dfn-cert: DFN-CERT-2023-1046
dfn-cert: DFN-CERT-2022-2439

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5778-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5778-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: xserver-xorg-core
Installed version: xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.5
Vulnerable package: xwayland
Installed version: xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xwayland-2:1.20.13-1ubuntu1~20.04.5

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 X.Org X Server extensions contained multiple security issues. 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-5778-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5778.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5778-1
cve: CVE-2022-4283
cve: CVE-2022-46340
cve: CVE-2022-46341

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-46342
cve: CVE-2022-46343
cve: CVE-2022-46344
advisory_id: USN-5778-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2022-2312
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-1046
dfn-cert: DFN-CERT-2023-0524
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2022-2859

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5378-2)

Summary
The remote host is missing an update for the 'xz-utils' package(s) announced via the USN-5378-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: xz-utils
Installed version: xz-utils-5.2.4-1ubuntu1
Fixed version: >=xz-utils-5.2.4-1ubuntu1.1

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

Affected Software/OS
'xz-utils' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Cleemy Desu Wayo discovered that XZ Utils incorrectly handled certain filenames. If a user or automated system were tricked into performing xzgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5378-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5378.2
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

```
url: https://ubuntu.com/security/notices/USN-5378-2
cve: CVE-2022-1271
advisory_id: USN-5378-2
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0034
cert-bund: CB-K22/0407
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2115
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0788
```

High (CVSS: 8.6)
NVT: Ubuntu: Security Advisory (USN-5907-1)

Summary
The remote host is missing an update for the 'c-ares' package(s) announced via the USN-5907-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libc-ares2
Installed version:    libc-ares2-1.15.0-1build1
Fixed version:      >=libc-ares2-1.15.0-1ubuntu0.2
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
It was discovered that c-ares incorrectly handled certain sortlist strings. A remote attacker could use this issue to cause c-ares to crash, resulting in 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-5907-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5907.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5907-1`
`cve: CVE-2022-4904`
`advisory_id: USN-5907-1`
`cert-bund: WID-SEC-2023-2817`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1614`
`dfn-cert: DFN-CERT-2023-2987`
`dfn-cert: DFN-CERT-2023-2772`
`dfn-cert: DFN-CERT-2023-2437`
`dfn-cert: DFN-CERT-2023-1591`
`dfn-cert: DFN-CERT-2023-1075`
`dfn-cert: DFN-CERT-2023-0799`
`dfn-cert: DFN-CERT-2023-0734`
`dfn-cert: DFN-CERT-2023-0407`

High (CVSS: 8.5)
NVT: Ubuntu: Security Advisory (USN-5772-1)

Summary
The remote host is missing an update for the 'qemu' package(s) announced via the USN-5772-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:    qemu
Installed version:     qemu-1:4.2-3ubuntu6.16
Fixed version:      >=qemu-1:4.2-3ubuntu6.24
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'qemu' 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 QEMU incorrectly handled bulk transfers from SPICE clients. A remote attacker could use this issue to cause QEMU to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. (CVE-2021-3682)
It was discovered that QEMU did not properly manage memory when it transfers the USB packets. A malicious guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2021-3750)
It was discovered that the QEMU SCSI device emulation incorrectly handled certain MODE SELECT commands. An attacker inside the guest could possibly use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. (CVE-2021-3930)
It was discovered that QEMU did not properly manage memory when it processing repeated messages to cancel the current SCSI request. A malicious privileged guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service. (CVE-2022-0216)
It was discovered that QEMU did not properly manage memory when it using Tulip device emulation. A malicious guest attacker could use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 22.10. (CVE-2022-2962)
It was discovered that QEMU did not properly manage memory when processing ClientCutText messages. A attacker could use this issue to cause QEMU to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3165)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5772-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5772.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5772-1`
`cve: CVE-2021-3682`
`cve: CVE-2021-3750`
`cve: CVE-2021-3930`
`cve: CVE-2022-0216`
`cve: CVE-2022-2962`
`cve: CVE-2022-3165`
`advisory_id: USN-5772-1`
`cert-bund: WID-SEC-2022-1728`
`cert-bund: WID-SEC-2022-1535`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1204
cert-bund: WID-SEC-2022-1158
cert-bund: WID-SEC-2022-1141
cert-bund: WID-SEC-2022-1122
cert-bund: WID-SEC-2022-1118
cert-bund: CB-K22/0618
cert-bund: CB-K21/1160
cert-bund: CB-K21/1026
cert-bund: CB-K21/0836
dfn-cert: DFN-CERT-2024-1079
dfn-cert: DFN-CERT-2024-0959
dfn-cert: DFN-CERT-2024-0277
dfn-cert: DFN-CERT-2024-0234
dfn-cert: DFN-CERT-2023-2869
dfn-cert: DFN-CERT-2023-2495
dfn-cert: DFN-CERT-2023-2305
dfn-cert: DFN-CERT-2023-2236
dfn-cert: DFN-CERT-2023-1991
dfn-cert: DFN-CERT-2023-1268
dfn-cert: DFN-CERT-2023-1117
dfn-cert: DFN-CERT-2023-1042
dfn-cert: DFN-CERT-2023-0626
dfn-cert: DFN-CERT-2023-0610
dfn-cert: DFN-CERT-2023-0591
dfn-cert: DFN-CERT-2023-0568
dfn-cert: DFN-CERT-2023-0526
dfn-cert: DFN-CERT-2023-0295
dfn-cert: DFN-CERT-2023-0171
dfn-cert: DFN-CERT-2022-2812
dfn-cert: DFN-CERT-2022-2570
dfn-cert: DFN-CERT-2022-2527
dfn-cert: DFN-CERT-2022-2398
dfn-cert: DFN-CERT-2022-2336
dfn-cert: DFN-CERT-2022-2303
dfn-cert: DFN-CERT-2022-2284
dfn-cert: DFN-CERT-2022-2234
dfn-cert: DFN-CERT-2022-1946
dfn-cert: DFN-CERT-2022-1824
dfn-cert: DFN-CERT-2022-0802
dfn-cert: DFN-CERT-2022-0751
dfn-cert: DFN-CERT-2022-0662
dfn-cert: DFN-CERT-2022-0459
dfn-cert: DFN-CERT-2022-0445
dfn-cert: DFN-CERT-2022-0006
dfn-cert: DFN-CERT-2021-2665
dfn-cert: DFN-CERT-2021-2569
dfn-cert: DFN-CERT-2021-2508

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2309
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2065
dfn-cert: DFN-CERT-2021-2046
dfn-cert: DFN-CERT-2021-1858
dfn-cert: DFN-CERT-2021-1824
dfn-cert: DFN-CERT-2021-1790

High (CVSS: 8.4)
NVT: Ubuntu: Security Advisory (USN-5240-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-aws-5.11, linux-azure, linux-azure-5.4, linux-azure-5.11, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gcp-5.11, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oem-5.10, linux-oem-5.13, linux-oem-5.14, linux-oracle, linux-oracle-5.4, linux-oracle-5.11, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5240-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.96.100

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-aws-5.11, linux-azure, linux-azure-5.4, linux-azure-5.11, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gcp-5.11, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oem-5.10, linux-oem-5.13, linux-oem-5.14, linux-oracle, linux-oracle-5.4, linux-oracle-5.11, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
William Liu and Jamie Hill-Daniel discovered that the file system context functionality in the Linux kernel contained an integer underflow vulnerability, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5240-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5240.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5240-1
cve: CVE-2022-0185
advisory_id: USN-5240-1
cert-bund: WID-SEC-2022-2061
cert-bund: WID-SEC-2022-0515
cert-bund: CB-K22/0059
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-0738
dfn-cert: DFN-CERT-2022-0368
dfn-cert: DFN-CERT-2022-0354
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0251
dfn-cert: DFN-CERT-2022-0237
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0186
dfn-cert: DFN-CERT-2022-0162
dfn-cert: DFN-CERT-2022-0141
dfn-cert: DFN-CERT-2022-0133
dfn-cert: DFN-CERT-2022-0127

High (CVSS: 8.2)
NVT: Ubuntu: Security Advisory (USN-6259-1)

Summary

The remote host is missing an update for the 'open-iscsi' package(s) announced via the USN-6259-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: open-iscsi
Installed version: open-iscsi-2.0.874-7.1ubuntu6.2
Fixed version: >=open-iscsi-2.0.874-7.1ubuntu6.4

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'open-iscsi' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Jos Wetzels, Stanislav Dashevskyi, and Amine Amri discovered that Open-iSCSI incorrectly handled certain checksums for IP packets. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-13987)
Jos Wetzels, Stanislav Dashevskyi, Amine Amri discovered that Open-iSCSI incorrectly handled certain parsing TCP MSS options. An attacker could possibly use this issue to cause a crash or cause unexpected behavior. (CVE-2020-13988)
Amine Amri and Stanislav Dashevskyi discovered that Open-iSCSI incorrectly handled certain TCP data. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-17437)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6259-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6259.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6259-1`
`cve: CVE-2020-13987`
`cve: CVE-2020-13988`
`cve: CVE-2020-17437`
`advisory_id: USN-6259-1`
`cert-bund: WID-SEC-2022-1044`
`cert-bund: CB-K20/1208`
`dfn-cert: DFN-CERT-2023-1730`
`dfn-cert: DFN-CERT-2022-1856`
`dfn-cert: DFN-CERT-2021-0118`

High (CVSS: 8.2)
NVT: Ubuntu: Security Advisory (USN-5622-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi' package(s) announced via the USN-5622-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:    linux-image-generic
Installed version:     linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.126.127
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of- bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33655)
Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information. (CVE-2022-1012, CVE-2022-32296)
Norbert Slusarek discovered that a race condition existed in the perf subsystem in the Linux kernel, resulting in a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1729)
It was discovered that the device-mapper verity (dm-verity) driver in the Linux kernel did not properly verify targets being loaded into the device- mapper table. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-2503)
Domingo Dirutigliano and Nicola Guerrera discovered that the netfilter subsystem in the Linux kernel did not properly handle rules that truncated packets below the packet header size. When such rules are in place, a remote attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-36946)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5622-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5622.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5622-1`
`cve: CVE-2021-33655`
`cve: CVE-2022-1012`
`cve: CVE-2022-1729`
`cve: CVE-2022-2503`
`cve: CVE-2022-32296`
`cve: CVE-2022-36946`
`advisory_id: USN-5622-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0841`
`cert-bund: WID-SEC-2023-0574`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1508
cert-bund: WID-SEC-2022-0845
cert-bund: WID-SEC-2022-0734
cert-bund: WID-SEC-2022-0501
cert-bund: WID-SEC-2022-0299
cert-bund: WID-SEC-2022-0180
cert-bund: CB-K22/0641
dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2023-2482
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2023-0503
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2649
dfn-cert: DFN-CERT-2022-2621
dfn-cert: DFN-CERT-2022-2619
dfn-cert: DFN-CERT-2022-2617
dfn-cert: DFN-CERT-2022-2616
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2448
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2358
dfn-cert: DFN-CERT-2022-2357
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2291
dfn-cert: DFN-CERT-2022-2277
dfn-cert: DFN-CERT-2022-2275
dfn-cert: DFN-CERT-2022-2273
dfn-cert: DFN-CERT-2022-2238
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2022-2174
dfn-cert: DFN-CERT-2022-2172
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2135
dfn-cert: DFN-CERT-2022-2103
dfn-cert: DFN-CERT-2022-2102
dfn-cert: DFN-CERT-2022-2101
dfn-cert: DFN-CERT-2022-2100
dfn-cert: DFN-CERT-2022-2078
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2063
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-2040
dfn-cert: DFN-CERT-2022-1969
dfn-cert: DFN-CERT-2022-1967
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2022-1960
dfn-cert: DFN-CERT-2022-1951
dfn-cert: DFN-CERT-2022-1930
dfn-cert: DFN-CERT-2022-1907
dfn-cert: DFN-CERT-2022-1888
dfn-cert: DFN-CERT-2022-1879
dfn-cert: DFN-CERT-2022-1867
dfn-cert: DFN-CERT-2022-1866
dfn-cert: DFN-CERT-2022-1847
dfn-cert: DFN-CERT-2022-1828
dfn-cert: DFN-CERT-2022-1823
dfn-cert: DFN-CERT-2022-1822
dfn-cert: DFN-CERT-2022-1816
dfn-cert: DFN-CERT-2022-1795
dfn-cert: DFN-CERT-2022-1794
dfn-cert: DFN-CERT-2022-1771
dfn-cert: DFN-CERT-2022-1769
dfn-cert: DFN-CERT-2022-1768
dfn-cert: DFN-CERT-2022-1767
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1702
dfn-cert: DFN-CERT-2022-1701
dfn-cert: DFN-CERT-2022-1660
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1622
dfn-cert: DFN-CERT-2022-1619
dfn-cert: DFN-CERT-2022-1604
dfn-cert: DFN-CERT-2022-1598
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1552

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1510
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1475
dfn-cert: DFN-CERT-2022-1439
dfn-cert: DFN-CERT-2022-1437
dfn-cert: DFN-CERT-2022-1436
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1419
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1397
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1312
dfn-cert: DFN-CERT-2022-1279
dfn-cert: DFN-CERT-2022-1165

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5078-1)

Summary
The remote host is missing an update for the 'squashfs-tools' package(s) announced via the USN-5078-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: squashfs-tools
Installed version: squashfs-tools-1:4.4-1
Fixed version: >=squashfs-tools-1:4.4-1ubuntu0.2

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

Affected Software/OS
'squashfs-tools' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Richard Weinberger discovered that Squashfs-Tools mishandled certain malformed SQUASHFS files. An attacker could use this vulnerability to write arbitrary files to the filesystem.

... 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-5078-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5078.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5078-1`
`cve: CVE-2021-41072`
`advisory_id: USN-5078-1`
`cert-bund: WID-SEC-2024-0995`
`dfn-cert: DFN-CERT-2024-1156`
`dfn-cert: DFN-CERT-2023-2807`
`dfn-cert: DFN-CERT-2021-1929`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-6473-2)

Summary
The remote host is missing an update for the 'python-pip' package(s) announced via the USN-6473-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python-pip-whl
Installed version:    python-pip-whl-20.0.2-5ubuntu1.5
Fixed version:      >=python-pip-whl-20.0.2-5ubuntu1.10
Vulnerable package:   python3-pip
Installed version:    python3-pip-20.0.2-5ubuntu1.5
Fixed version:      >=python3-pip-20.0.2-5ubuntu1.10
```

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

Affected Software/OS
'python-pip' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
USN-6473-1 fixed vulnerabilities in urllib3. This update provides the corresponding updates for the urllib3 module bundled into pip.
Original advisory details:

... continues on next page ...

... continued from previous page ...

It was discovered that urllib3 didn't strip HTTP Authorization header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-25091)
It was discovered that urllib3 didn't strip HTTP Cookie header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-43804)
It was discovered that urllib3 didn't strip HTTP body on status code 303 redirects under certain circumstances. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-45803)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6473-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6473.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6473-2`
`cve: CVE-2018-25091`
`cve: CVE-2023-43804`
`cve: CVE-2023-45803`
`advisory_id: USN-6473-2`
`cert-bund: WID-SEC-2024-1228`
`cert-bund: WID-SEC-2024-1003`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0423`
`cert-bund: WID-SEC-2023-3146`
`cert-bund: WID-SEC-2023-3025`
`cert-bund: WID-SEC-2023-2964`
`cert-bund: WID-SEC-2023-2862`
`dfn-cert: DFN-CERT-2024-1392`
`dfn-cert: DFN-CERT-2024-1391`
`dfn-cert: DFN-CERT-2024-1384`
`dfn-cert: DFN-CERT-2024-1382`
`dfn-cert: DFN-CERT-2024-1380`
`dfn-cert: DFN-CERT-2024-0744`
`dfn-cert: DFN-CERT-2024-0598`
`dfn-cert: DFN-CERT-2024-0312`
`dfn-cert: DFN-CERT-2024-0073`
`dfn-cert: DFN-CERT-2023-3204`
`dfn-cert: DFN-CERT-2023-3160`
`dfn-cert: DFN-CERT-2023-2914`
`dfn-cert: DFN-CERT-2023-2724`
`dfn-cert: DFN-CERT-2023-2714`
`dfn-cert: DFN-CERT-2023-2563`
`dfn-cert: DFN-CERT-2023-2421`
`dfn-cert: DFN-CERT-2023-2366`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-6473-1)

Summary
The remote host is missing an update for the 'python-urllib3' package(s) announced via the USN-6473-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-urllib3
Installed version:    python3-urllib3-1.25.8-2ubuntu0.1
Fixed version:      >=python3-urllib3-1.25.8-2ubuntu0.3
```

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

Affected Software/OS
'python-urllib3' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that urllib3 didn't strip HTTP Authorization header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-25091)
It was discovered that urllib3 didn't strip HTTP Cookie header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-43804)
It was discovered that urllib3 didn't strip HTTP body on status code 303 redirects under certain circumstances. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-45803)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6473-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6473.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6473-1
cve: CVE-2018-25091
cve: CVE-2023-43804
cve: CVE-2023-45803
advisory_id: USN-6473-1
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-1003
cert-bund: WID-SEC-2024-0794
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0423
cert-bund: WID-SEC-2023-3146
cert-bund: WID-SEC-2023-3025
cert-bund: WID-SEC-2023-2964
cert-bund: WID-SEC-2023-2862
dfn-cert: DFN-CERT-2024-1392
dfn-cert: DFN-CERT-2024-1391
dfn-cert: DFN-CERT-2024-1384
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0598
dfn-cert: DFN-CERT-2024-0312
dfn-cert: DFN-CERT-2024-0073
dfn-cert: DFN-CERT-2023-3204
dfn-cert: DFN-CERT-2023-3160
dfn-cert: DFN-CERT-2023-2914
dfn-cert: DFN-CERT-2023-2724
dfn-cert: DFN-CERT-2023-2714
dfn-cert: DFN-CERT-2023-2563
dfn-cert: DFN-CERT-2023-2421
dfn-cert: DFN-CERT-2023-2366

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5691-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5691-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.131.131

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

David Bouman and Billy Jheng Bing Jhong discovered that a race condition existed in the io_uring subsystem 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-2022-2602)

Sonke Huster discovered that an integer overflow vulnerability existed in the WiFi driver stack in the Linux kernel, leading to a buffer overflow. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-41674)

Sonke Huster discovered that the WiFi driver stack in the Linux kernel did not properly perform reference counting in some situations, 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-2022-42720)

Sonke Huster discovered that the WiFi driver stack in the Linux kernel did not properly handle BSSID/SSID lists in some situations. A physically proximate attacker could use this to cause a denial of service (infinite loop). (CVE-2022-42721)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5691-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5691.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5691-1`
`cve: CVE-2022-2602`
`cve: CVE-2022-41674`
`cve: CVE-2022-42720`
`cve: CVE-2022-42721`
`advisory_id: USN-5691-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0018`
`cert-bund: WID-SEC-2022-1792`
`cert-bund: WID-SEC-2022-1716`
`dfn-cert: DFN-CERT-2024-0603`
`dfn-cert: DFN-CERT-2023-1955`
`dfn-cert: DFN-CERT-2023-1116`
`dfn-cert: DFN-CERT-2023-1041`
`dfn-cert: DFN-CERT-2023-0553`
`dfn-cert: DFN-CERT-2023-0273`
`dfn-cert: DFN-CERT-2023-0260`
`dfn-cert: DFN-CERT-2023-0059`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0021
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2835
dfn-cert: DFN-CERT-2022-2611
dfn-cert: DFN-CERT-2022-2599
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2449
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2442
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2334
dfn-cert: DFN-CERT-2022-2333
dfn-cert: DFN-CERT-2022-2332
dfn-cert: DFN-CERT-2022-2326
dfn-cert: DFN-CERT-2022-2298
dfn-cert: DFN-CERT-2022-2295
dfn-cert: DFN-CERT-2022-2292
dfn-cert: DFN-CERT-2022-2265
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5078-3)

Summary
The remote host is missing an update for the 'squashfs-tools' package(s) announced via the USN-5078-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   squashfs-tools
Installed version:    squashfs-tools-1:4.4-1
Fixed version:      >=squashfs-tools-1:4.4-1ubuntu0.3
```

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

Affected Software/OS
'squashfs-tools' package(s) on Ubuntu 20.04, Ubuntu 21.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
USN-5078-1 fixed a vulnerability in Squashfs-Tools. That update was incomplete and could still result in Squashfs-Tools mishandling certain malformed SQUASHFS files. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Richard Weinberger discovered that Squashfs-Tools mishandled certain malformed SQUASHFS files. An attacker could use this vulnerability to write arbitrary files to the filesystem.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5078-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5078.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5078-3`
`cve: CVE-2021-41072`
`advisory_id: USN-5078-3`
`cert-bund: WID-SEC-2024-0995`
`dfn-cert: DFN-CERT-2024-1156`
`dfn-cert: DFN-CERT-2023-2807`
`dfn-cert: DFN-CERT-2021-1929`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5068-1)

Summary
The remote host is missing an update for the 'libgd2' package(s) announced via the USN-5068-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libgd3
Installed version:    libgd3-2.2.5-5.2ubuntu2
Fixed version:      >=libgd3-2.2.5-5.2ubuntu2.1
```

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

Affected Software/OS
'libgd2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that GD Graphics Library incorrectly handled certain GD and GD2 files. An attacker could possibly use this issue to cause a crash or expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, Ubuntu 16.04 ESM, and Ubuntu 14.04 ESM. (CVE-2017-6363)
It was discovered that GD Graphics Library incorrectly handled certain TGA files. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2021-381)
It was discovered that GD Graphics Library incorrectly handled certain files. An attacker could possibly use this issue to cause a crash. (CVE-2021-40145)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5068-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5068.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5068-1`
`cve: CVE-2017-6363`
`cve: CVE-2021-38115`
`cve: CVE-2021-40145`
`advisory_id: USN-5068-1`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`dfn-cert: DFN-CERT-2024-0902`
`dfn-cert: DFN-CERT-2021-2185`
`dfn-cert: DFN-CERT-2021-1930`
`dfn-cert: DFN-CERT-2021-1894`
`dfn-cert: DFN-CERT-2020-1078`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-6112-2)

Summary
The remote host is missing an update for the 'perl' package(s) announced via the USN-6112-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   perl
Installed version:    perl-5.30.0-9ubuntu0.2
Fixed version:      >=perl-5.30.0-9ubuntu0.4
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'perl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
USN-6112-1 fixed vulnerabilities in Perl. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04.
Original advisory details:
It was discovered that Perl was not properly verifying TLS certificates when using CPAN together with HTTP::Tiny to download modules over HTTPS. If a remote attacker were able to intercept communications, this flaw could potentially be used to install altered modules.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6112-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6112.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6112-2`
`cve: CVE-2023-31484`
`advisory_id: USN-6112-2`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0257`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-1608`
`dfn-cert: DFN-CERT-2024-1283`
`dfn-cert: DFN-CERT-2023-2542`
`dfn-cert: DFN-CERT-2023-2490`
`dfn-cert: DFN-CERT-2023-1225`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-6618-1)

Summary
The remote host is missing an update for the 'pillow' package(s) announced via the USN-6618-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  python3-pil`

... continues on next page ...

... continued from previous page ...

```
Installed version:    python3-pil-7.0.0-4ubuntu0.4
Fixed version:      >=python3-pil-7.0.0-4ubuntu0.8
```

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

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

Vulnerability Insight
It was discovered that Pillow incorrectly handled certain long text arguments. An attacker could possibly use this issue to cause Pillow to consume resources, leading to a denial of service. This issue only affected Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2023-44271)
Duarte Santos discovered that Pillow incorrectly handled the environment parameter to PIL.ImageMath.eval. An attacker could possibly use this issue to execute arbitrary code. (CVE-2023-50447)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6618-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6618.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6618-1`
`cve: CVE-2023-44271`
`cve: CVE-2023-50447`
`advisory_id: USN-6618-1`
`cert-bund: WID-SEC-2024-1328`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0873`
`cert-bund: WID-SEC-2024-0522`
`cert-bund: WID-SEC-2024-0423`
`cert-bund: WID-SEC-2024-0337`
`cert-bund: WID-SEC-2024-0184`
`dfn-cert: DFN-CERT-2024-1483`
`dfn-cert: DFN-CERT-2024-0767`
`dfn-cert: DFN-CERT-2024-0284`
`dfn-cert: DFN-CERT-2024-0258`
`dfn-cert: DFN-CERT-2024-0190`
`dfn-cert: DFN-CERT-2023-2731`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5404-1)

Summary
The remote host is missing an update for the 'rsyslog' package(s) announced via the USN-5404-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   rsyslog
Installed version:    rsyslog-8.2001.0-1ubuntu1.1
Fixed version:      >=rsyslog-8.2001.0-1ubuntu1.3
```

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

Affected Software/OS
'rsyslog' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Pieter Agten discovered that Rsyslog incorrectly handled certain requests. An attacker could possibly use this issue to cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5404-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5404.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5404-1
cve: CVE-2022-24903
advisory_id: USN-5404-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1790
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-0123
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1167
dfn-cert: DFN-CERT-2022-1020
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5638-2)

Summary
The remote host is missing an update for the 'expat' package(s) announced via the USN-5638-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.2.9-1build1
Fixed version:      >=libexpat1-2.2.9-1ubuntu0.5
```

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

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

Vulnerability Insight
USN-5638-1 fixed a vulnerability in Expat. This update provides the corresponding updates for Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.
It was discovered that Expat incorrectly handled memory in out-of-memory situations. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS. (CVE-2022-43680)
Original advisory details:
Rhodri James discovered that Expat incorrectly handled memory when processing certain malformed XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5638-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5638.2
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5638-2
cve: CVE-2022-40674
cve: CVE-2022-43680
advisory_id: USN-5638-2
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-3226
cert-bund: WID-SEC-2023-2676
cert-bund: WID-SEC-2023-1818
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1807
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0292
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2055
cert-bund: WID-SEC-2022-1844
cert-bund: WID-SEC-2022-1504
dfn-cert: DFN-CERT-2023-3223
dfn-cert: DFN-CERT-2023-1919
dfn-cert: DFN-CERT-2023-1651
dfn-cert: DFN-CERT-2023-1648
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0666
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0269
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2821
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2664
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2575
dfn-cert: DFN-CERT-2022-2566
dfn-cert: DFN-CERT-2022-2480
dfn-cert: DFN-CERT-2022-2408
dfn-cert: DFN-CERT-2022-2344
dfn-cert: DFN-CERT-2022-2343
dfn-cert: DFN-CERT-2022-2264
dfn-cert: DFN-CERT-2022-2218
dfn-cert: DFN-CERT-2022-2207
dfn-cert: DFN-CERT-2022-2120

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5397-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5397-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.10
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.10
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.10
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Patrick Monnerat discovered that curl incorrectly handled certain OAUTH2. An attacker could possibly use this issue to access sensitive information. (CVE-2022-22576)
Harry Sintonen discovered that curl incorrectly handled certain requests. An attacker could possibly use this issue to expose sensitive information. (CVE-2022-27774, CVE-2022-27775, CVE-2022-27776)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5397-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5397.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5397-1
cve: CVE-2022-22576
cve: CVE-2022-27774
cve: CVE-2022-27775
cve: CVE-2022-27776
advisory_id: USN-5397-1
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-0826
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0733
cert-bund: WID-SEC-2022-0649
cert-bund: WID-SEC-2022-0522
cert-bund: WID-SEC-2022-0393
cert-bund: CB-K22/0505
dfn-cert: DFN-CERT-2023-1142
dfn-cert: DFN-CERT-2023-0214
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2594
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1937
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1553
dfn-cert: DFN-CERT-2022-1490
dfn-cert: DFN-CERT-2022-1454
dfn-cert: DFN-CERT-2022-0935
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5047-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5047-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-91.0.1+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that Firefox could be made to incorrectly accept newlines in HTTP/3 response headers. If a user were tricked into opening a specially crafted website, an attacker could exploit this to conduct header splitting attacks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5047-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5047.1
Version used: `2024-02-02T04:09:01Z`

References
`advisory_id: USN-5047-1`
`url: https://ubuntu.com/security/notices/USN-5047-1`
`cve: CVE-2021-29991`
`cert-bund: CB-K21/0884`
`dfn-cert: DFN-CERT-2021-1762`

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5057-1)

Summary
The remote host is missing an update for the 'squashfs-tools' package(s) announced via the USN-5057-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   squashfs-tools
Installed version:    squashfs-tools-1:4.4-1
Fixed version:      >=squashfs-tools-1:4.4-1ubuntu0.1
```

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

Affected Software/OS
'squashfs-tools' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Etienne Stalmans discovered that Squashfs-Tools mishandled certain malformed SQUASHFS files. An attacker could use this vulnerability to write arbitrary files to the filesystem.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5057-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2021.5057.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5057-1
cve: CVE-2021-40153
advisory_id: USN-5057-1
cert-bund: WID-SEC-2024-0995
dfn-cert: DFN-CERT-2024-1156
dfn-cert: DFN-CERT-2023-2807
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1830

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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libavcodec58
Installed version:    libavcodec58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavcodec58-7:4.2.7-0ubuntu0.1+esm1
Vulnerable package:   libavformat58
Installed version:    libavformat58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavformat58-7:4.2.7-0ubuntu0.1+esm1
Vulnerable package:   libavutil56
Installed version:    libavutil56-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavutil56-7:4.2.7-0ubuntu0.1+esm1
Vulnerable package:   libpostproc55
Installed version:    libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version:      >=libpostproc55-7:4.2.7-0ubuntu0.1+esm1
Vulnerable package:   libswresample3
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1+esm1
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1+esm1
```

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

... continues on next page ...

... continued from previous page ...

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 22.04 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
Version used: `2024-02-02T04:09:01Z`

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-2023-1355`
`dfn-cert: DFN-CERT-2023-1028`
`dfn-cert: DFN-CERT-2023-0789`
`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-6726-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-6726-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.176.174
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
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)
Dan Carpenter discovered that the netfilter subsystem in the Linux kernel did not store data in properly sized memory locations. A local user could use this to cause a denial of service (system crash). (CVE-2024-0607)
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: - Architecture specifics, - Cryptographic API, - Android drivers, - EDAC drivers, - GPU drivers, - Media drivers, - MTD block device drivers, - Network drivers, - NVME drivers, - TTY drivers, - Userspace I/O drivers, - F2FS file system, - GFS2 file system, - IPv6 Networking, - AppArmor security module, (CVE-2023-52464, CVE-2023-52448, CVE-2023-52457, CVE-2023-52443, CVE-2023-52439, CVE-2023-52612, CVE-2024-26633, CVE-2024-26597, CVE-2023-52449, CVE-2023-52444, CVE-2023-52609, CVE-2023-52469, CVE-2023-52445, CVE-2023-52451, CVE-2023-52470, CVE-2023-52454, CVE-2023-52436, CVE-2023-52438)

... 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-6726-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2024.6726.1

Version used: `2024-04-18T04:09:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-6726-1
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-2023-52443
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-2023-52457
cve: CVE-2023-52464
cve: CVE-2023-52469
cve: CVE-2023-52470
cve: CVE-2023-52609
cve: CVE-2023-52612
cve: CVE-2024-0607
cve: CVE-2024-23851
cve: CVE-2024-26597
cve: CVE-2024-26633
advisory_id: USN-6726-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0654
cert-bund: WID-SEC-2024-0475
cert-bund: WID-SEC-2024-0473
cert-bund: WID-SEC-2024-0444
cert-bund: WID-SEC-2024-0345
cert-bund: WID-SEC-2024-0177
cert-bund: WID-SEC-2024-0176
cert-bund: WID-SEC-2024-0135
dfn-cert: DFN-CERT-2024-1512
dfn-cert: DFN-CERT-2024-1478
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1351
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1337
dfn-cert: DFN-CERT-2024-1309
dfn-cert: DFN-CERT-2024-1307
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1202
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-2024-1060
dfn-cert: DFN-CERT-2024-1059
dfn-cert: DFN-CERT-2024-1057
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-2024-0973
dfn-cert: DFN-CERT-2024-0972
dfn-cert: DFN-CERT-2024-0971
dfn-cert: DFN-CERT-2024-0949
dfn-cert: DFN-CERT-2024-0946
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-2024-0750
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-2024-0630
dfn-cert: DFN-CERT-2024-0611
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

... continues on next page ...

... continued from previous page ...

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

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6741-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6741-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.177.175

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

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, - BPF subsystem, - Netfilter, (CVE-2023-52603, CVE-2023-52600, CVE-2024-26581, CVE-2024-26589)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6741-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6741.1
Version used: 2024-04-22T04:09:21Z

References

url: https://ubuntu.com/security/notices/USN-6741-1
cve: CVE-2023-24023
cve: CVE-2023-52600
cve: CVE-2023-52603
cve: CVE-2024-26581
cve: CVE-2024-26589
advisory_id: USN-6741-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0561
cert-bund: WID-SEC-2024-0473
cert-bund: WID-SEC-2024-0444
cert-bund: WID-SEC-2023-3043
cert-bund: WID-SEC-2023-2890
dfn-cert: DFN-CERT-2024-1512
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
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-2024-0924
dfn-cert: DFN-CERT-2024-0773
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-2023-2820

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6767-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6767-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.181.179
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
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)
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: - ARM64 architecture, - PowerPC architecture, - S390 architecture, - Block layer subsystem, - Android drivers, - Hardware random number generator core, - GPU drivers, - Hardware monitoring drivers, - I2C subsystem, - IIO Magnetometer sensors drivers, - InfiniBand drivers, - Network drivers, - PCI driver for MicroSemi Switchtec, - PHY drivers, - Ceph distributed file system, - Ext4 file system, - JFS file system, - NILFS2 file system, - Pstore file system, - Core kernel, - Memory management, - CAN network layer, - Networking core, - IPv4 networking, - Logical Link layer, - Netfilter, - NFC subsystem, - SMC sockets, - Sun RPC protocol, - TIPC protocol, - Realtek audio codecs, (CVE-2024-26696, CVE-2023-52583, CVE-2024-26720, CVE-2023-52615, CVE-2023-52599, CVE-2023-52587, CVE-2024-26635, CVE-2024-26704, CVE-2024-26625, CVE-2024-26825, CVE-2023-52622, CVE-2023-52435, CVE-2023-52617, CVE-2023-52598, CVE-2024-26645, CVE-2023-52619, CVE-2024-26593, CVE-2024-26685, CVE-2023-52602, CVE-2023-52486, CVE-2024-26697, CVE-2024-26675, CVE-2024-26600, CVE-2023-52604, CVE-2024-26664, CVE-2024-26606, CVE-2023-52594, CVE-2024-26671, CVE-2024-26598, CVE-2024-26673, CVE-2024-26920, CVE-2024-26722, CVE-2023-52601, CVE-2024-26602, CVE-2023-52637, CVE-2023-52623, CVE-2024-26702, CVE-2023-52597, CVE-2024-26684, CVE-2023-52606, CVE-2024-26679, CVE-2024-26663, CVE-2024-26910, CVE-2024-26615, CVE-2023-52595, CVE-2023-52607, CVE-2024-26636)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6767-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6767.1
Version used: `2024-05-08T04:07:32Z`

References

`url: https://ubuntu.com/security/notices/USN-6767-1`
`cve: CVE-2023-52435`
`cve: CVE-2023-52486`
`cve: CVE-2023-52583`
`cve: CVE-2023-52587`
`cve: CVE-2023-52594`
`cve: CVE-2023-52595`
`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-2023-52615`
`cve: CVE-2023-52617`
`cve: CVE-2023-52619`
`cve: CVE-2023-52622`
`cve: CVE-2023-52623`
`cve: CVE-2023-52637`
`cve: CVE-2024-23849`
`cve: CVE-2024-26593`
`cve: CVE-2024-26598`
`cve: CVE-2024-26600`
`cve: CVE-2024-26602`
`cve: CVE-2024-26606`
`cve: CVE-2024-26615`
`cve: CVE-2024-26625`
`cve: CVE-2024-26635`
`cve: CVE-2024-26636`
`cve: CVE-2024-26645`
`cve: CVE-2024-26663`
`cve: CVE-2024-26664`
`cve: CVE-2024-26671`
`cve: CVE-2024-26673`
`cve: CVE-2024-26675`
`cve: CVE-2024-26679`
`cve: CVE-2024-26684`
`cve: CVE-2024-26685`
`cve: CVE-2024-26696`

... continues on next page ...

... continued from previous page ...

cve: CVE-2024-26697
cve: CVE-2024-26702
cve: CVE-2024-26704
cve: CVE-2024-26720
cve: CVE-2024-26722
cve: CVE-2024-26825
cve: CVE-2024-26910
cve: CVE-2024-26920
advisory_id: USN-6767-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0920
cert-bund: WID-SEC-2024-0913
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-2024-0594
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-2024-0444
cert-bund: WID-SEC-2024-0177
dfn-cert: DFN-CERT-2024-1552
dfn-cert: DFN-CERT-2024-1541
dfn-cert: DFN-CERT-2024-1537
dfn-cert: DFN-CERT-2024-1518
dfn-cert: DFN-CERT-2024-1508
dfn-cert: DFN-CERT-2024-1495
dfn-cert: DFN-CERT-2024-1478
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1437
dfn-cert: DFN-CERT-2024-1400
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1338
dfn-cert: DFN-CERT-2024-1337
dfn-cert: DFN-CERT-2024-1327
dfn-cert: DFN-CERT-2024-1309
dfn-cert: DFN-CERT-2024-1307
dfn-cert: DFN-CERT-2024-1304
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

... continues on next page ...

... continued from previous page ...

```
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-2024-0924
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-2024-0295
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6831-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6831-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.186.184
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

It was discovered that the HugeTLB file system component of the Linux Kernel contained a NULL pointer dereference vulnerability. A privileged attacker could possibly use this to to cause a denial of service. (CVE-2024-0841)

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: - ARM32 architecture, - PowerPC architecture, - x86 architecture, - DMA engine subsystem, - EFI core, - GPU drivers, - InfiniBand drivers, - Multiple devices driver, - Network drivers, - Power supply drivers, - TCM subsystem, - Userspace I/O drivers, - USB subsystem, - Framebuffer layer, - AFS file system, - File systems infrastructure, - BTRFS file system, - Ext4 file system, - Bluetooth subsystem, - Networking core, - IPv4 networking, - IPv6 networking, - L2TP protocol, - MAC80211 subsystem, - Netfilter, - Netlink, - Wireless networking, (CVE-2024-26748, CVE-2024-27417, CVE-2024-26840, CVE-2023-52504, CVE-2024-26790, CVE-2024-26763, CVE-2024-26805, CVE-2024-26773, CVE-2021-47063, CVE-2024-26791, CVE-2024-27413, CVE-2024-26788, CVE-2024-27405, CVE-2024-26845, CVE-2024-26766, CVE-2021-47070, CVE-2024-26839, CVE-2024-26712, CVE-2024-27412, CVE-2024-26752, CVE-2024-26778, CVE-2024-26735, CVE-2024-26736, CVE-2024-27410, CVE-2024-26779, CVE-2024-26804, CVE-2024-26749, CVE-2024-26793, CVE-2024-26764, CVE-2024-26751, CVE-2024-35811, CVE-2024-26835, CVE-2024-26772, CVE-2024-26777, CVE-2024-26688, CVE-2024-27416, CVE-2024-26801, CVE-2024-26733, CVE-2024-27414, CVE-2024-26754, CVE-2024-26848)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6831-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2024.6831.1

Version used: `2024-06-13T04:07:56Z`

References

`url: https://ubuntu.com/security/notices/USN-6831-1`
`cve: CVE-2021-47063`
`cve: CVE-2021-47070`
`cve: CVE-2023-52504`
`cve: CVE-2024-0841`
`cve: CVE-2024-26688`
`cve: CVE-2024-26712`
`cve: CVE-2024-26733`
`cve: CVE-2024-26735`
`cve: CVE-2024-26736`
`cve: CVE-2024-26748`
`cve: CVE-2024-26749`
`cve: CVE-2024-26751`

... continues on next page ...

... continued from previous page ...

cve: CVE-2024-26752
cve: CVE-2024-26754
cve: CVE-2024-26763
cve: CVE-2024-26764
cve: CVE-2024-26766
cve: CVE-2024-26772
cve: CVE-2024-26773
cve: CVE-2024-26777
cve: CVE-2024-26778
cve: CVE-2024-26779
cve: CVE-2024-26788
cve: CVE-2024-26790
cve: CVE-2024-26791
cve: CVE-2024-26793
cve: CVE-2024-26801
cve: CVE-2024-26804
cve: CVE-2024-26805
cve: CVE-2024-26835
cve: CVE-2024-26839
cve: CVE-2024-26840
cve: CVE-2024-26845
cve: CVE-2024-26848
cve: CVE-2024-27405
cve: CVE-2024-27410
cve: CVE-2024-27412
cve: CVE-2024-27413
cve: CVE-2024-27414
cve: CVE-2024-27416
cve: CVE-2024-27417
cve: CVE-2024-35811
advisory_id: USN-6831-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1188
cert-bund: WID-SEC-2024-0920
cert-bund: WID-SEC-2024-0803
cert-bund: WID-SEC-2024-0773
cert-bund: WID-SEC-2024-0534
cert-bund: WID-SEC-2024-0527
cert-bund: WID-SEC-2024-0232
dfn-cert: DFN-CERT-2024-1553
dfn-cert: DFN-CERT-2024-1552
dfn-cert: DFN-CERT-2024-1518
dfn-cert: DFN-CERT-2024-1508
dfn-cert: DFN-CERT-2024-1496
dfn-cert: DFN-CERT-2024-1478
dfn-cert: DFN-CERT-2024-1477
dfn-cert: DFN-CERT-2024-1448

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1437
dfn-cert: DFN-CERT-2024-1400
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1376
dfn-cert: DFN-CERT-2024-1375
dfn-cert: DFN-CERT-2024-1351
dfn-cert: DFN-CERT-2024-1347
dfn-cert: DFN-CERT-2024-1346
dfn-cert: DFN-CERT-2024-1338
dfn-cert: DFN-CERT-2024-1337
dfn-cert: DFN-CERT-2024-1327
dfn-cert: DFN-CERT-2024-1315
dfn-cert: DFN-CERT-2024-1312
dfn-cert: DFN-CERT-2024-1309
dfn-cert: DFN-CERT-2024-1308
dfn-cert: DFN-CERT-2024-1307
dfn-cert: DFN-CERT-2024-1305
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1303
dfn-cert: DFN-CERT-2024-1302
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1122
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

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6160-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-6160-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: binutils
Installed version: binutils-2.34-6ubuntu1.1
Fixed version: >=binutils-2.34-6ubuntu1.6

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'binutils' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that GNU binutils incorrectly performed bounds checking operations when parsing stabs debugging information. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6160-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6160.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6160-1`
`cve: CVE-2021-45078`
`advisory_id: USN-6160-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-1124`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`dfn-cert: DFN-CERT-2022-2655`
`dfn-cert: DFN-CERT-2022-0661`
`dfn-cert: DFN-CERT-2021-2646`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6581-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-6581-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   binutils
Installed version:    binutils-2.34-6ubuntu1.1
Fixed version:      >=binutils-2.34-6ubuntu1.8
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
It was discovered that GNU binutils was not properly performing bounds checks in several functions, which could lead to a buffer overflow. An attacker could possibly use this issue to cause a denial of service, expose sensitive information or execute arbitrary code. (CVE-2022-44840, CVE-2022-45703)
It was discovered that GNU binutils incorrectly handled memory management operations in several of its functions, which could lead to excessive memory consumption due to memory leaks. An attacker could possibly use these issues to cause a denial of service. (CVE-2022-47007, CVE-2022-47008, CVE-2022-47010, CVE-2022-47011)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6581-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6581.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6581-1`
`cve: CVE-2022-44840`
`cve: CVE-2022-45703`
`cve: CVE-2022-47007`
`cve: CVE-2022-47008`
`cve: CVE-2022-47010`
`cve: CVE-2022-47011`
`advisory_id: USN-6581-1`
`cert-bund: WID-SEC-2023-2165`
`dfn-cert: DFN-CERT-2024-0107`
`dfn-cert: DFN-CERT-2023-2386`
`dfn-cert: DFN-CERT-2023-2222`
`dfn-cert: DFN-CERT-2023-2183`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5463-1)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5463-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   ntfs-3g
Installed version:    ntfs-3g-1:2017.3.23AR.3-3ubuntu1
Fixed version:      >=ntfs-3g-1:2017.3.23AR.3-3ubuntu1.2
```

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that NTFS-3G incorrectly handled the ntfsck tool. If a user or automated system were tricked into using ntfsck on a specially crafted disk image, a remote attacker could possibly use this issue to execute arbitrary code. (CVE-2021-46790)
Roman Fiedler discovered that NTFS-3G incorrectly handled certain return codes. A local attacker could possibly use this issue to intercept protocol traffic between FUSE and the kernel. (CVE-2022-30783)
It was discovered that NTFS-3G incorrectly handled certain NTFS disk images. If a user or automated system were tricked into mounting a specially crafted disk image, a remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-30784, CVE-2022-30786, CVE-2022-30788, CVE-2022-30789)
Roman Fiedler discovered that NTFS-3G incorrectly handled certain file handles. A local attacker could possibly use this issue to read and write arbitrary memory. (CVE-2022-30785, CVE-2022-30787)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5463-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5463.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5463-1
cve: CVE-2021-46790
cve: CVE-2022-30783
cve: CVE-2022-30784
cve: CVE-2022-30785
cve: CVE-2022-30786
cve: CVE-2022-30787
cve: CVE-2022-30788
cve: CVE-2022-30789
advisory_id: USN-5463-1
cert-bund: WID-SEC-2023-1185
dfn-cert: DFN-CERT-2023-1117
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1048
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1218
dfn-cert: DFN-CERT-2022-1217

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5711-1)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5711-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: ntfs-3g
Installed version: ntfs-3g-1:2017.3.23AR.3-3ubuntu1
Fixed version: >=ntfs-3g-1:2017.3.23AR.3-3ubuntu1.3

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
Yuchen Zeng and Eduardo Vela discovered that NTFS-3G incorrectly validated certain NTFS metadata. A local attacker could possibly use this issue to gain privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5711-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5711.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5711-1
cve: CVE-2022-40284
advisory_id: USN-5711-1
cert-bund: WID-SEC-2023-2780
dfn-cert: DFN-CERT-2024-0234
dfn-cert: DFN-CERT-2023-2215
dfn-cert: DFN-CERT-2022-2457

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5578-1)

Summary
The remote host is missing an update for the 'open-vm-tools' package(s) announced via the USN-5578-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   open-vm-tools
Installed version:    open-vm-tools-2:11.2.5-2ubuntu1~ubuntu20.04.1
Fixed version:      >=open-vm-tools-2:11.3.0-2ubuntu0~ubuntu20.04.3
```

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

Affected Software/OS
'open-vm-tools' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that Open VM Tools incorrectly handled certain requests. An attacker inside the guest could possibly use this issue to gain root privileges inside the virtual machine.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5578-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5578.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5578-1
cve: CVE-2022-31676
advisory_id: USN-5578-1
cert-bund: WID-SEC-2022-1159
dfn-cert: DFN-CERT-2022-1873
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5680-1)

Summary
The remote host is missing an update for the 'gthumb' package(s) announced via the USN-5680-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   gthumb
Installed version:    gthumb-3:3.8.0-2.1build1
Fixed version:      >=gthumb-3:3.8.0-2.1ubuntu0.1
Vulnerable package:   gthumb-data
Installed version:    gthumb-data-3:3.8.0-2.1build1
Fixed version:      >=gthumb-data-3:3.8.0-2.1ubuntu0.1
```

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

Affected Software/OS
'gthumb' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that gThumb did not properly managed memory when processing certain image files. If a user were tricked into opening a specially crafted JPEG file, an attacker could possibly use this issue to cause gThumb to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2019-20326)
It was discovered that gThumb did not properly handled certain malformed image files. If a user were tricked into opening a specially crafted JPEG file, an attacker could possibly use this issue to cause gThumb to crash, resulting in a denial of service. (CVE-2020-36427)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5680-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5680.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5680-1
cve: CVE-2019-20326
cve: CVE-2020-36427
advisory_id: USN-5680-1
dfn-cert: DFN-CERT-2022-2272
dfn-cert: DFN-CERT-2020-0068
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5064-1)

Summary
The remote host is missing an update for the 'cpio' package(s) announced via the USN-5064-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: cpio
Installed version: cpio-2.13+dfsg-2
Fixed version: >=cpio-2.13+dfsg-2ubuntu0.3

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

Affected Software/OS
'cpio' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Maverick Chung and Qiaoyi Fang discovered that cpio incorrectly handled certain pattern files. A remote attacker could use this issue to cause cpio to crash, resulting in 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-5064-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5064.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5064-1
cve: CVE-2021-38185
advisory_id: USN-5064-1
cert-bund: WID-SEC-2022-1852
dfn-cert: DFN-CERT-2023-1271
dfn-cert: DFN-CERT-2021-1738

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5555-1)

Summary
The remote host is missing an update for the 'gst-plugins-good1.0' package(s) announced via the USN-5555-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: gstreamer1.0-plugins-good

... continues on next page ...

... continued from previous page ...

Installed version: gstreamer1.0-plugins-good-1.16.2-1ubuntu2.1
Fixed version: >=gstreamer1.0-plugins-good-1.16.3-0ubuntu1.1

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

Affected Software/OS
'gst-plugins-good1.0' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-1920, CVE-2022-1921)
It was discovered that GStreamer Good Plugins incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1922, CVE-2022-1923, CVE-2022-1924, CVE-2022-1925, CVE-2022-2122)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5555-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5555.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5555-1
cve: CVE-2022-1920
cve: CVE-2022-1921
cve: CVE-2022-1922
cve: CVE-2022-1923
cve: CVE-2022-1924
cve: CVE-2022-1925
cve: CVE-2022-2122
advisory_id: USN-5555-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0374
dfn-cert: DFN-CERT-2023-2206
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-1753

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5366-1)

Summary
The remote host is missing an update for the 'fribidi' package(s) announced via the USN-5366-1 advisory.

... continues on next page ...

. . . continued from previous page . . .

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libfribidi0
Installed version: libfribidi0-1.0.8-2
Fixed version: >=libfribidi0-1.0.8-2ubuntu0.1

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

Affected Software/OS
'fribidi' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that FriBidi incorrectly handled processing of input strings resulting in memory corruption. An attacker could use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25308)
It was discovered that FriBidi incorrectly validated input data to its CapRTL unicode encoder, resulting in memory corruption. An attacker could use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25309)
It was discovered that FriBidi incorrectly handled empty input when removing marks from unicode strings, resulting in a crash. An attacker could use this to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25310)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5366-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5366.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5366-1
cve: CVE-2022-25308
cve: CVE-2022-25309
cve: CVE-2022-25310
advisory_id: USN-5366-1
cert-bund: WID-SEC-2022-2044
dfn-cert: DFN-CERT-2022-0699

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5554-1)

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'gdk-pixbuf' package(s) announced via the USN-5554-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgdk-pixbuf2.0-0
Installed version:    libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.2
Fixed version:      >=libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.3
```

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

Affected Software/OS
'gdk-pixbuf' package(s) on Ubuntu 20.04.

Vulnerability Insight
Pedro Ribeiro discovered that the GDK-PixBuf library did not properly handle certain GIF images. If an user or automated system were tricked into opening a specially crafted GIF file, a remote attacker could use this flaw to cause GDK-PixBuf to crash, resulting in 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-5554-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5554.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5554-1
cve: CVE-2021-46829
advisory_id: USN-5554-1
cert-bund: WID-SEC-2023-1185
dfn-cert: DFN-CERT-2022-1996
dfn-cert: DFN-CERT-2022-1747
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6708-1)

Summary
The remote host is missing an update for the 'graphviz' package(s) announced via the USN-6708-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: graphviz
Installed version: graphviz-2.42.2-3build2
Fixed version: >=graphviz-2.42.2-3ubuntu0.1~esm2

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

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

Vulnerability Insight
It was discovered that Graphviz incorrectly handled certain config6a files. 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-6708-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6708.1
Version used: 2024-03-22T04:08:37Z

References
url: https://ubuntu.com/security/notices/USN-6708-1
cve: CVE-2023-46045
advisory_id: USN-6708-1
dfn-cert: DFN-CERT-2024-0765

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6806-1)

Summary
The remote host is missing an update for the 'gdk-pixbuf' package(s) announced via the USN-6806-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgdk-pixbuf2.0-0
Installed version: libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.2
Fixed version: >=libgdk-pixbuf2.0-0-2.40.0+dfsg-3ubuntu0.5

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'gdk-pixbuf' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Pedro Ribeiro and Vitor Pedreira discovered that the GDK-PixBuf library did not properly handle certain ANI files. An attacker could use this flaw to cause GDK-PixBuf to crash, resulting in a denial of service, or to possibly execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6806-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6806.1
Version used: `2024-06-06T04:07:45Z`

References
`url: https://ubuntu.com/security/notices/USN-6806-1`
`cve: CVE-2022-48622`
`advisory_id: USN-6806-1`
`cert-bund: WID-SEC-2024-0233`
`dfn-cert: DFN-CERT-2024-1356`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6165-1)

Summary
The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-6165-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.64.6-1~ubuntu20.04.3
Fixed version:      >=libglib2.0-0-2.64.6-1~ubuntu20.04.6
Vulnerable package:   libglib2.0-bin
Installed version:    libglib2.0-bin-2.64.6-1~ubuntu20.04.3
Fixed version:      >=libglib2.0-bin-2.64.6-1~ubuntu20.04.6
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'glib2.0' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that GLib incorrectly handled non-normal GVariants. An attacker could use this issue to cause GLib to crash, resulting in a denial of service, or perform other unknown attacks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6165-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6165.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6165-1`
`cve: CVE-2023-24593`
`cve: CVE-2023-25180`
`cve: CVE-2023-29499`
`cve: CVE-2023-32611`
`cve: CVE-2023-32636`
`cve: CVE-2023-32643`
`cve: CVE-2023-32665`
`advisory_id: USN-6165-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2853`
`cert-bund: WID-SEC-2023-2825`
`dfn-cert: DFN-CERT-2024-1167`
`dfn-cert: DFN-CERT-2024-0285`
`dfn-cert: DFN-CERT-2023-3124`
`dfn-cert: DFN-CERT-2023-2270`
`dfn-cert: DFN-CERT-2023-2074`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-1379`
`dfn-cert: DFN-CERT-2023-1322`
`dfn-cert: DFN-CERT-2023-0903`
`dfn-cert: DFN-CERT-2023-0770`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6050-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-6050-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.25.1-1ubuntu3.1
Fixed version: >=git-1:2.25.1-1ubuntu3.11

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

Affected Software/OS
'git' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Git incorrectly handled certain commands. An attacker could possibly use this issue to overwriting some paths. (CVE-2023-25652)
Maxime Escourbiac and Yassine BENGANA discovered that Git incorrectly handled some gettext machinery. An attacker could possibly use this issue to allows the malicious placement of crafted messages. (CVE-2023-25815)
Andre Baptista and Vitor Pinho discovered that Git incorrectly handled certain configurations. An attacker could possibly use this issue to arbitrary configuration injection. (CVE-2023-29007)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6050-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6050.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6050-1
cve: CVE-2023-25652
cve: CVE-2023-25815
cve: CVE-2023-29007
advisory_id: USN-6050-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1446
cert-bund: WID-SEC-2023-1072
dfn-cert: DFN-CERT-2023-2837
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1359
dfn-cert: DFN-CERT-2023-1177

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1175
dfn-cert: DFN-CERT-2023-0964

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5230-1)

Summary
The remote host is missing an update for the 'cpanminus' package(s) announced via the USN-5230-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: cpanminus
Installed version: cpanminus-1.7044-1
Fixed version: >=cpanminus-1.7044-1ubuntu0.1~esm1

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

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

Vulnerability Insight
It was discovered that App::cpanminus did not properly verify CHECKSUMS files. An attacker could possibly use this issue to bypass signature verification, gaining access to sensitive data or possibly executing unauthorized code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5230-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5230.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5230-1
cve: CVE-2020-16154
advisory_id: USN-5230-1
dfn-cert: DFN-CERT-2022-0234

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5811-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'sudo' package(s) announced via the USN-5811-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   sudo
Installed version:    sudo-1.8.31-1ubuntu1.2
Fixed version:      >=sudo-1.8.31-1ubuntu1.4
```

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

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

Vulnerability Insight
Matthieu Barjole and Victor Cutillas discovered that Sudo incorrectly handled user-specified editors when using the sudoedit command. A local attacker that has permission to use the sudoedit command could possibly use this issue to edit arbitrary files. (CVE-2023-22809)
It was discovered that the Protobuf-c library, used by Sudo, incorrectly handled certain arithmetic shifts. An attacker could possibly use this issue to cause Sudo to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-33070)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5811-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5811.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5811-1
cve: CVE-2022-33070
cve: CVE-2023-22809
advisory_id: USN-5811-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1348
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0266
cert-bund: WID-SEC-2023-0151
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0423
dfn-cert: DFN-CERT-2023-0129
dfn-cert: DFN-CERT-2022-1658

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5511-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5511-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.25.1-1ubuntu3.1
Fixed version: >=git-1:2.25.1-1ubuntu3.5

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

Affected Software/OS
'git' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Carlo Marcelo Arenas Belon discovered that an issue related to CVE-2022-24765 still affected Git. An attacker could possibly use this issue to run arbitrary commands as administrator. (CVE-2022-29187)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5511-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5511.1
Version used: 2024-02-28T10:02:42Z

References
url: https://ubuntu.com/security/notices/USN-5511-1
cve: CVE-2022-29187
advisory_id: USN-5511-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0664

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0228
dfn-cert: DFN-CERT-2022-2848
dfn-cert: DFN-CERT-2022-2445
dfn-cert: DFN-CERT-2022-2197
dfn-cert: DFN-CERT-2022-2057
dfn-cert: DFN-CERT-2022-1566

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5193-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5193-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: xserver-xorg-core
Installed version: xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.2

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 21.04, Ubuntu 21.10.

Vulnerability Insight
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5193-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5193.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5193-1
cve: CVE-2021-4008
cve: CVE-2021-4009
cve: CVE-2021-4010

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-4011
advisory_id: USN-5193-1
cert-bund: WID-SEC-2023-0192
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: CB-K21/1278
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2658
dfn-cert: DFN-CERT-2021-2612

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5376-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5376-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.25.1-1ubuntu3.1
Fixed version: >=git-1:2.25.1-1ubuntu3.3

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

Affected Software/OS
'git' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Yu Chen Dong discovered that Git incorrectly handled certain repository paths in platforms with multiple users support. An attacker could possibly use this issue to run arbitrary commands.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5376-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5376.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5376-1
cve: CVE-2022-24765

... continues on next page ...

... continued from previous page ...

```
advisory_id: USN-5376-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0252
cert-bund: CB-K22/0433
cert-bund: CB-K22/0429
dfn-cert: DFN-CERT-2024-0228
dfn-cert: DFN-CERT-2022-2848
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2197
dfn-cert: DFN-CERT-2022-2057
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1113
dfn-cert: DFN-CERT-2022-0822
dfn-cert: DFN-CERT-2022-0815
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5382-1)

Summary
The remote host is missing an update for the 'libinput' package(s) announced via the USN-5382-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libinput10
Installed version:    libinput10-1.15.5-1ubuntu0.2
Fixed version:      >=libinput10-1.15.5-1ubuntu0.3
```

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

Affected Software/OS
'libinput' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Albin Eldstal-Ahrens and Lukas Lamster discovered libinput did not properly handle input devices with specially crafted names. A local attacker with physical access could use this to cause libinput to crash or expose sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5382-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5382.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5382-1
cve: CVE-2022-1215
advisory_id: USN-5382-1
cert-bund: WID-SEC-2022-0525
dfn-cert: DFN-CERT-2022-0894

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6364-1)

Summary
The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-6364-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ghostscript
Installed version:    ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version:      >=ghostscript-9.50~dfsg-5ubuntu4.10
Vulnerable package:   libgs9
Installed version:    libgs9-9.50~dfsg-5ubuntu4.2
Fixed version:      >=libgs9-9.50~dfsg-5ubuntu4.10
```

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

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

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled certain PDF files. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-21710)
It was discovered that Ghostscript incorrectly handled certain PDF files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-21890)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6364-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6364.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-6364-1
cve: CVE-2020-21710
cve: CVE-2020-21890
advisory_id: USN-6364-1
cert-bund: WID-SEC-2023-2353
dfn-cert: DFN-CERT-2024-1387
dfn-cert: DFN-CERT-2023-2148

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5510-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5510-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: xserver-xorg-core
Installed version: xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.3
Vulnerable package: xwayland
Installed version: xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version: >=xwayland-2:1.20.13-1ubuntu1~20.04.3

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 21.10, Ubuntu 22.04.

Vulnerability Insight
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5510-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5510.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-5510-1
cve: CVE-2022-2319
cve: CVE-2022-2320
advisory_id: USN-5510-1
cert-bund: WID-SEC-2022-0661
dfn-cert: DFN-CERT-2022-1556

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5331-2)

Summary
The remote host is missing an update for the 'tcpdump' package(s) announced via the USN-5331-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: tcpdump
Installed version: tcpdump-4.9.3-4
Fixed version: >=tcpdump-4.9.3-4ubuntu0.1

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

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

Vulnerability Insight
USN-5331-1 fixed several vulnerabilities in tcpdump. This update provides the corresponding update for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.
Original advisory details: It was discovered that tcpdump incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2018-16301)
It was discovered that tcpdump incorrectly handled certain captured data. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-8037)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5331-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5331.2
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-5331-2
cve: CVE-2018-16301
cve: CVE-2020-8037
advisory_id: USN-5331-2
cert-bund: WID-SEC-2022-2281
cert-bund: WID-SEC-2022-0571
cert-bund: CB-K21/1164
cert-bund: CB-K21/0446
cert-bund: CB-K19/1065
dfn-cert: DFN-CERT-2022-0612
dfn-cert: DFN-CERT-2022-0399
dfn-cert: DFN-CERT-2021-0868
dfn-cert: DFN-CERT-2021-0867
dfn-cert: DFN-CERT-2021-0866
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2020-2531
dfn-cert: DFN-CERT-2020-2460
dfn-cert: DFN-CERT-2020-0782
dfn-cert: DFN-CERT-2019-2621
dfn-cert: DFN-CERT-2019-2153
dfn-cert: DFN-CERT-2019-2143
dfn-cert: DFN-CERT-2019-2128
dfn-cert: DFN-CERT-2019-2080

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6213-1)

Summary

The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-6213-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: ghostscript
Installed version: ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version: >=ghostscript-9.50~dfsg-5ubuntu4.8

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'ghostscript' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled pipe devices. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6213-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6213.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6213-1`
`cve: CVE-2023-36664`
`advisory_id: USN-6213-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-1580`
`dfn-cert: DFN-CERT-2023-1526`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5380-1)

Summary
The remote host is missing an update for the 'bash' package(s) announced via the USN-5380-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   bash
Installed version:    bash-5.0-6ubuntu1.1
Fixed version:      >=bash-5.0-6ubuntu1.2
```

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

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

Vulnerability Insight
It was discovered that Bash did not properly drop privileges when the binary had the setuid bit enabled. An attacker could possibly use this issue to escalate privileges.

... 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-5380-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5380.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5380-1`
`cve: CVE-2019-18276`
`advisory_id: USN-5380-1`
`cert-bund: WID-SEC-2024-0054`
`cert-bund: WID-SEC-2022-1908`
`cert-bund: CB-K21/0537`
`dfn-cert: DFN-CERT-2024-0059`
`dfn-cert: DFN-CERT-2021-1066`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5244-2)

Summary
The remote host is missing an update for the 'dbus' package(s) announced via the USN-5244-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   dbus
Installed version:    dbus-1.12.16-2ubuntu2.1
Fixed version:      >=dbus-1.12.16-2ubuntu2.2
Vulnerable package:   libdbus-1-3
Installed version:    libdbus-1-3-1.12.16-2ubuntu2.1
Fixed version:      >=libdbus-1-3-1.12.16-2ubuntu2.2
```

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

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

Vulnerability Insight
USN-5244-1 fixed a vulnerability in DBus. This update provides the corresponding update for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.
Original advisory details:

... continues on next page ...

... continued from previous page ...

Daniel Onaca discovered that DBus contained a use-after-free vulnerability, caused by the incorrect handling of usernames sharing the same UID. An attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5244-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5244.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5244-2`
`cve: CVE-2020-35512`
`advisory_id: USN-5244-2`
`cert-bund: WID-SEC-2022-1012`
`cert-bund: CB-K21/0179`
`dfn-cert: DFN-CERT-2021-1569`
`dfn-cert: DFN-CERT-2021-1421`

High (CVSS: 7.8)
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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.6
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.6
```

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

... continues on next page ...

... continued from previous page ...

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: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5846-1`
`cve: CVE-2023-0494`
`advisory_id: USN-5846-1`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-0293`
`dfn-cert: DFN-CERT-2023-1230`
`dfn-cert: DFN-CERT-2023-1046`
`dfn-cert: DFN-CERT-2023-0277`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5986-1)

Summary
The remote host is missing an update for the 'xorg-server, xorg-server-hwe-18.04, xwayland' package(s) announced via the USN-5986-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.8
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.8
```

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.

... continues on next page ...

... continued from previous page ...

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-5986-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5986.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5986-1`
`cve: CVE-2023-1393`
`advisory_id: USN-5986-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-0793`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-0706`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6453-1)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6453-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.9
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.9
```

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

Affected Software/OS
'xorg-server, xwayland' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled prepending values to certain properties. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-5367)
Sri discovered that the X.Org X Server incorrectly handled detroying windows in certain legacy multi-screen setups. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-5380)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6453-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6453.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6453-1`
`cve: CVE-2023-5367`
`cve: CVE-2023-5380`
`advisory_id: USN-6453-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1092`
`cert-bund: WID-SEC-2023-2749`
`cert-bund: WID-SEC-2023-2735`
`dfn-cert: DFN-CERT-2024-1393`
`dfn-cert: DFN-CERT-2024-1383`
`dfn-cert: DFN-CERT-2024-1161`
`dfn-cert: DFN-CERT-2024-1149`
`dfn-cert: DFN-CERT-2024-1145`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2024-0012`
`dfn-cert: DFN-CERT-2023-2926`
`dfn-cert: DFN-CERT-2023-2913`
`dfn-cert: DFN-CERT-2023-2625`
`dfn-cert: DFN-CERT-2023-2622`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6555-1)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6555-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  xserver-xorg-core`
`Installed version:  xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2`

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.12
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.12
```

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

Affected Software/OS
'xorg-server, xwayland' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled XKB button actions. An attacker could possibly use this issue to cause the X Server to crash, execute arbitrary code, or escalate privileges. (CVE-2023-6377)
Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled memory when processing the RRChangeOutputProperty and RRChangeProviderProperty APIs. An attacker could possibly use this issue to cause the X Server to crash, or obtain sensitive information. (CVE-2023-6478)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6555-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6555.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6555-1
cve: CVE-2023-6377
cve: CVE-2023-6478
advisory_id: USN-6555-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-3131
dfn-cert: DFN-CERT-2024-1393
dfn-cert: DFN-CERT-2024-1149
dfn-cert: DFN-CERT-2024-1145
dfn-cert: DFN-CERT-2024-0012
dfn-cert: DFN-CERT-2023-3115
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5119-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'libcaca' package(s) announced via the USN-5119-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libcaca0
Installed version:    libcaca0-0.99.beta19-2.1ubuntu1.20.04.1
Fixed version:      >=libcaca0-0.99.beta19-2.1ubuntu1.20.04.2
```

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

Affected Software/OS
'libcaca' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that libcaca incorrectly handled certain images. An attacker could possibly use this issue to cause a crash. (CVE-2021-30498, CVE-2021-30499)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5119-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5119.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5119-1
cve: CVE-2021-30498
cve: CVE-2021-30499
advisory_id: USN-5119-1
dfn-cert: DFN-CERT-2022-0607
dfn-cert: DFN-CERT-2022-0523
dfn-cert: DFN-CERT-2021-2219
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6166-1)

Summary
The remote host is missing an update for the 'libcap2' package(s) announced via the USN-6166-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   libcap2
Installed version:    libcap2-1:2.32-1
Fixed version:      >=libcap2-1:2.32-1ubuntu0.1
Vulnerable package:   libcap2-bin
Installed version:    libcap2-bin-1:2.32-1
Fixed version:      >=libcap2-bin-1:2.32-1ubuntu0.1
```

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

Affected Software/OS
'libcap2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
David Gstir discovered that libcap2 incorrectly handled certain return codes. An attacker could possibly use this issue to cause libcap2 to consume memory, leading to a denial of service. (CVE-2023-2602)
Richard Weinberger discovered that libcap2 incorrectly handled certain long input strings. An attacker could use this issue to cause libcap2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-2603)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6166-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6166.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6166-1
cve: CVE-2023-2602
cve: CVE-2023-2603
advisory_id: USN-6166-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2017
dfn-cert: DFN-CERT-2023-1939
dfn-cert: DFN-CERT-2023-1687
dfn-cert: DFN-CERT-2023-1380
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5423-1)

Summary
The remote host is missing an update for the 'clamav' package(s) announced via the USN-5423-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   clamav
Installed version:    clamav-0.103.2+dfsg-0ubuntu0.20.04.2
Fixed version:      >=clamav-0.103.6+dfsg-0ubuntu0.20.04.1
```

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

Affected Software/OS
'clamav' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Michal Dardas discovered that ClamAV incorrectly handled parsing CHM files. A remote attacker could possibly use this issue to cause ClamAV to stop responding, resulting in a denial of service. (CVE-2022-20770)
Michal Dardas discovered that ClamAV incorrectly handled parsing TIFF files. A remote attacker could possibly use this issue to cause ClamAV to stop responding, resulting in a denial of service. (CVE-2022-20771)
Michal Dardas discovered that ClamAV incorrectly handled parsing HTML files. A remote attacker could possibly use this issue to cause ClamAV to consume resources, resulting in a denial of service. (CVE-2022-20785)
Michal Dardas discovered that ClamAV incorrectly handled loading the signature database. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-20792)
Alexander Patrakov and Antoine Gatineau discovered that ClamAV incorrectly handled the scan verdict cache check. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service, or possibly execute arbitrary code.(CVE-2022-20796)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5423-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5423.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5423-1
cve: CVE-2022-20770
```

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2022-20771
cve: CVE-2022-20785
cve: CVE-2022-20792
cve: CVE-2022-20796
advisory_id: USN-5423-1
cert-bund: WID-SEC-2022-0122
cert-bund: CB-K22/0546
dfn-cert: DFN-CERT-2022-2652
dfn-cert: DFN-CERT-2022-0998
dfn-cert: DFN-CERT-2022-0997

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5476-1)

Summary
The remote host is missing an update for the 'liblouis' package(s) announced via the USN-5476-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: liblouis20
Installed version: liblouis20-3.12.0-3
Fixed version: >=liblouis20-3.12.0-3ubuntu0.1

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

Affected Software/OS
'liblouis' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Han Zheng discovered that Liblouis incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. This issue was addressed in Ubuntu 21.10 and Ubuntu 22.04 LTS. (CVE-2022-26981)
It was discovered that Liblouis incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash. (CVE-2022-31783)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5476-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5476.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-5476-1
cve: CVE-2022-26981
cve: CVE-2022-31783
advisory_id: USN-5476-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0782
cert-bund: WID-SEC-2022-0778
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-1633
dfn-cert: DFN-CERT-2022-1631
dfn-cert: DFN-CERT-2022-1299

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5459-1)

Summary

The remote host is missing an update for the 'cifs-utils' package(s) announced via the USN-5459-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: cifs-utils
Installed version: cifs-utils-2:6.9-1ubuntu0.1
Fixed version: >=cifs-utils-2:6.9-1ubuntu0.2

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'cifs-utils' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight

Aurelien Aptel discovered that cifs-utils invoked a shell when requesting a password. In certain environments, a local attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-14342)

It was discovered that cifs-utils incorrectly used host credentials when mounting a krb5 CIFS file system from within a container. An attacker inside a container could possibly use this issue to obtain access to sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2021-20208)

... continues on next page ...

... continued from previous page ...

It was discovered that cifs-utils incorrectly handled certain command-line arguments. A local attacker could possibly use this issue to obtain root privileges. (CVE-2022-27239)
It was discovered that cifs-utils incorrectly handled verbose logging. A local attacker could possibly use this issue to obtain sensitive information. (CVE-2022-29869)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5459-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5459.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5459-1`
`cve: CVE-2020-14342`
`cve: CVE-2021-20208`
`cve: CVE-2022-27239`
`cve: CVE-2022-29869`
`advisory_id: USN-5459-1`
`dfn-cert: DFN-CERT-2022-1815`
`dfn-cert: DFN-CERT-2022-1409`
`dfn-cert: DFN-CERT-2022-1267`
`dfn-cert: DFN-CERT-2022-1251`
`dfn-cert: DFN-CERT-2022-0965`
`dfn-cert: DFN-CERT-2022-0943`
`dfn-cert: DFN-CERT-2021-0918`
`dfn-cert: DFN-CERT-2021-0741`
`dfn-cert: DFN-CERT-2020-2069`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5483-1)

Summary
The remote host is missing an update for the 'exempi' package(s) announced via the USN-5483-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libexempi8
Installed version:    libexempi8-2.5.1-1build1
Fixed version:      >=libexempi8-2.5.1-1ubuntu0.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'exempi' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that Exempi incorrectly handled certain media files. If a user or automated system were tricked into opening a specially crafted file, a remote attacker could cause Exempi to stop responding or crash, resulting in 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-5483-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5483.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5483-1`
`cve: CVE-2018-12648`
`cve: CVE-2021-36045`
`cve: CVE-2021-36046`
`cve: CVE-2021-36047`
`cve: CVE-2021-36048`
`cve: CVE-2021-36050`
`cve: CVE-2021-36051`
`cve: CVE-2021-36052`
`cve: CVE-2021-36053`
`cve: CVE-2021-36054`
`cve: CVE-2021-36055`
`cve: CVE-2021-36056`
`cve: CVE-2021-36058`
`cve: CVE-2021-36064`
`cve: CVE-2021-39847`
`cve: CVE-2021-40716`
`cve: CVE-2021-40732`
`cve: CVE-2021-42528`
`cve: CVE-2021-42529`
`cve: CVE-2021-42530`
`cve: CVE-2021-42531`
`cve: CVE-2021-42532`
`advisory_id: USN-5483-1`
`cert-bund: CB-K21/0975`
`dfn-cert: DFN-CERT-2023-2272`
`dfn-cert: DFN-CERT-2022-1363`
`dfn-cert: DFN-CERT-2018-1956`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5464-1)

Summary
The remote host is missing an update for the 'e2fsprogs' package(s) announced via the USN-5464-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   e2fsprogs
Installed version:    e2fsprogs-1.45.5-2ubuntu1
Fixed version:      >=e2fsprogs-1.45.5-2ubuntu1.1
```

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

Affected Software/OS
'e2fsprogs' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Nils Bars discovered that e2fsprogs incorrectly handled certain file systems. A local attacker could use this issue with a crafted file system image to possibly execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5464-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5464.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5464-1
cve: CVE-2022-1304
advisory_id: USN-5464-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-0179
cert-bund: CB-K22/0616
dfn-cert: DFN-CERT-2023-2442
dfn-cert: DFN-CERT-2022-1091
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6698-1)

. . . continues on next page . . .

... continued from previous page ...

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6698-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:    vim
Installed version:     vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.22
```

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 23.10.

Vulnerability Insight
Zhen Zhou discovered that Vim did not properly manage memory. 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-6698-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6698.1
Version used: `2024-03-19T04:08:52Z`

References
```
url: https://ubuntu.com/security/notices/USN-6698-1
cve: CVE-2024-22667
advisory_id: USN-6698-1
cert-bund: WID-SEC-2024-0291
dfn-cert: DFN-CERT-2024-0608
dfn-cert: DFN-CERT-2024-0346
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5606-1)

Summary
The remote host is missing an update for the 'poppler' package(s) announced via the USN-5606-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   libpoppler97
Installed version:    libpoppler97-0.86.1-0ubuntu1
Fixed version:      >=libpoppler97-0.86.1-0ubuntu1.1
Vulnerable package:   poppler-utils
Installed version:    poppler-utils-0.86.1-0ubuntu1
Fixed version:      >=poppler-utils-0.86.1-0ubuntu1.1
```

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

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

Vulnerability Insight
It was discovered that poppler incorrectly handled certain PDF. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5606-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5606.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5606-1
cve: CVE-2022-38784
advisory_id: USN-5606-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2022-1214
dfn-cert: DFN-CERT-2023-0438
dfn-cert: DFN-CERT-2022-2123
dfn-cert: DFN-CERT-2022-2009
dfn-cert: DFN-CERT-2022-1963
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5427-1)

Summary
The remote host is missing an update for the 'apport' package(s) announced via the USN-5427-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   apport
Installed version:    apport-2.20.11-0ubuntu27.18
Fixed version:      >=apport-2.20.11-0ubuntu27.24
Vulnerable package:   python3-apport
Installed version:    python3-apport-2.20.11-0ubuntu27.18
Fixed version:      >=python3-apport-2.20.11-0ubuntu27.24
```

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

Affected Software/OS
'apport' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Muqing Liu and neoni discovered that Apport incorrectly handled detecting if an executable was replaced after a crash. A local attacker could possibly use this issue to execute arbitrary code as the root user. (CVE-2021-3899)
Gerrit Venema discovered that Apport incorrectly handled connections to Apport sockets inside containers. A local attacker could possibly use this issue to connect to arbitrary sockets as the root user. (CVE-2022-1242)
Gerrit Venema discovered that Apport incorrectly handled user settings files. A local attacker could possibly use this issue to cause Apport to consume resources, leading to a denial of service. (CVE-2022-28652)
Gerrit Venema discovered that Apport did not limit the amount of logging from D-Bus connections. A local attacker could possibly use this issue to fill up the Apport log file, leading to denial of service. (CVE-2022-28654)
Gerrit Venema discovered that Apport did not filter D-Bus connection strings. A local attacker could possibly use this issue to cause Apport to make arbitrary network connections. (CVE-2022-28655)
Gerrit Venema discovered that Apport did not limit the amount of memory being consumed during D-Bus connections. A local attacker could possibly use this issue to cause Apport to consume memory, leading to a denial of service. (CVE-2022-28656)
Gerrit Venema discovered that Apport did not disable the python crash handler before chrooting into a container. A local attacker could possibly use this issue to execute arbitrary code. (CVE-2022-28657)
Gerrit Venema discovered that Apport incorrectly handled filename argument whitespace. A local attacker could possibly use this issue to spoof arguments to the Apport daemon. (CVE-2022-28658)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5427-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5427.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-06-12T04:07:57Z

References
cve: CVE-2022-1242
url: https://ubuntu.com/security/notices/USN-5427-1
cve: CVE-2021-3899
cve: CVE-2022-28652
cve: CVE-2022-28654
cve: CVE-2022-28655
cve: CVE-2022-28656
cve: CVE-2022-28657
cve: CVE-2022-28658
advisory_id: USN-5427-1
dfn-cert: DFN-CERT-2022-1124

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6137-1)

Summary
The remote host is missing an update for the 'libraw' package(s) announced via the USN-6137-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libraw19
Installed version: libraw19-0.19.5-1ubuntu1
Fixed version: >=libraw19-0.19.5-1ubuntu1.2

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

Affected Software/OS
'libraw' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that LibRaw incorrectly handled photo files. If a user or automated system were tricked into processing a specially crafted photo file, a remote attacker could cause applications linked against LibRaw to crash, resulting in 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-6137-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2023.6137.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6137-1
cve: CVE-2021-32142
cve: CVE-2023-1729
advisory_id: USN-6137-1
cert-bund: WID-SEC-2024-0995
cert-bund: WID-SEC-2023-2853
dfn-cert: DFN-CERT-2023-1219
dfn-cert: DFN-CERT-2023-1030
dfn-cert: DFN-CERT-2023-0456

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5291-1)

Summary
The remote host is missing an update for the 'libarchive' package(s) announced via the USN-5291-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libarchive13
Installed version: libarchive13-3.4.0-2ubuntu1
Fixed version: >=libarchive13-3.4.0-2ubuntu1.1

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

Affected Software/OS
'libarchive' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that libarchive incorrectly handled symlinks. If a user or automated system were tricked into processing a specially crafted archive, an attacker could possibly use this issue to change modes, times, ACLs, and flags on arbitrary files. (CVE-2021-23177, CVE-2021-31566) It was discovered that libarchive incorrectly handled certain RAR archives. If a user or automated system were tricked into processing a specially crafted RAR archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36976)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5291-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5291.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5291-1
cve: CVE-2021-23177
cve: CVE-2021-31566
cve: CVE-2021-36976
advisory_id: USN-5291-1
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1130
cert-bund: WID-SEC-2022-1056
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0045
cert-bund: CB-K22/0322
cert-bund: CB-K22/0317
cert-bund: CB-K22/0316
cert-bund: CB-K22/0030
cert-bund: CB-K21/0765
dfn-cert: DFN-CERT-2022-2548
dfn-cert: DFN-CERT-2022-2077
dfn-cert: DFN-CERT-2022-1253
dfn-cert: DFN-CERT-2022-0959
dfn-cert: DFN-CERT-2022-0680
dfn-cert: DFN-CERT-2022-0599
dfn-cert: DFN-CERT-2022-0589
dfn-cert: DFN-CERT-2022-0586
dfn-cert: DFN-CERT-2022-0385
dfn-cert: DFN-CERT-2022-0384
dfn-cert: DFN-CERT-2022-0052

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6018-1)

Summary

The remote host is missing an update for the 'apport' package(s) announced via the USN-6018-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: apport
Installed version: apport-2.20.11-0ubuntu27.18

... continues on next page ...

... continued from previous page ...

Fixed version: >=apport-2.20.11-0ubuntu27.26

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

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

Vulnerability Insight
Chen Lu, Lei Wang, and YiQi Sun discovered a privilege escalation vulnerability in apport-cli when viewing crash reports and unprivileged users are allowed to run sudo less. A local attacker on a specially configured system could use this to escalate their privilege.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6018-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6018.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6018-1
url: https://launchpad.net/bugs/2016023
cve: CVE-2023-1326
advisory_id: USN-6018-1
dfn-cert: DFN-CERT-2023-0851

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5274-1)

Summary
The remote host is missing an update for the 'libsdl2' package(s) announced via the USN-5274-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libsdl2-2.0-0
Installed version: libsdl2-2.0-0-2.0.10+dfsg1-3
Fixed version: >=libsdl2-2.0-0-2.0.10+dfsg1-3ubuntu0.1~esm1

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libsdl2' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that Simple DirectMedia Layer library incorrectly handled memory when parsing certain specially crafted .BMP files. An attacker could possibly use these issues to crash the application or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5274-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5274.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5274-1
cve: CVE-2020-14409
cve: CVE-2020-14410
advisory_id: USN-5274-1
dfn-cert: DFN-CERT-2023-0298
dfn-cert: DFN-CERT-2022-0917
dfn-cert: DFN-CERT-2022-0883
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0200
dfn-cert: DFN-CERT-2021-0196
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5023-1)

Summary
The remote host is missing an update for the 'aspell' package(s) announced via the USN-5023-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   aspell
Installed version:    aspell-0.60.8-1build1
Fixed version:      >=aspell-0.60.8-1ubuntu0.1
Vulnerable package:   libaspell15
Installed version:    libaspell15-0.60.8-1build1
Fixed version:      >=libaspell15-0.60.8-1ubuntu0.1
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'aspell' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Aspell incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5023-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5023.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5023-1`
`cve: CVE-2019-25051`
`advisory_id: USN-5023-1`
`cert-bund: WID-SEC-2023-1993`
`cert-bund: CB-K22/0557`
`dfn-cert: DFN-CERT-2021-1930`
`dfn-cert: DFN-CERT-2021-1728`
`dfn-cert: DFN-CERT-2021-1597`
`dfn-cert: DFN-CERT-2021-1550`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6471-1)

Summary
The remote host is missing an update for the 'libsndfile' package(s) announced via the USN-6471-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libsndfile1
Installed version:    libsndfile1-1.0.28-7
Fixed version:      >=libsndfile1-1.0.28-7ubuntu0.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libsndfile' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that libsndfile contained multiple arithmetic overflows. If a user or automated system were tricked into processing a specially crafted audio file, 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-6471-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6471.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6471-1`
`cve: CVE-2022-33065`
`advisory_id: USN-6471-1`
`cert-bund: WID-SEC-2023-1906`
`dfn-cert: DFN-CERT-2024-1413`
`dfn-cert: DFN-CERT-2023-2699`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6557-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6557-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.21
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.21
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.21
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'vim' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Vim could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1725)
It was discovered that Vim could be made to recurse infinitely. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1771)
It was discovered that Vim could be made to write out of bounds with a put command. 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. (CVE-2022-1886)
It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1897, CVE-2022-2000)
It was discovered that Vim did not properly manage memory in the spell command. 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. (CVE-2022-2042)
It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-46246, CVE-2023-48231)
It was discovered that Vim could be made to divide by zero. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-48232)
It was discovered that Vim contained multiple arithmetic overflows. An attacker could possibly use these issues to cause a denial of service. (CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237)
It was discovered that Vim did not properly manage memory in the substitute command. 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, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-48706)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6557-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6557.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6557-1`
`cve: CVE-2022-1725`
`cve: CVE-2022-1771`
`cve: CVE-2022-1886`
`cve: CVE-2022-1897`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-2000
cve: CVE-2022-2042
cve: CVE-2023-46246
cve: CVE-2023-48231
cve: CVE-2023-48232
cve: CVE-2023-48233
cve: CVE-2023-48234
cve: CVE-2023-48235
cve: CVE-2023-48236
cve: CVE-2023-48237
cve: CVE-2023-48706
advisory_id: USN-6557-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2997
cert-bund: WID-SEC-2023-2962
cert-bund: WID-SEC-2023-2757
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1566
cert-bund: WID-SEC-2022-0369
cert-bund: WID-SEC-2022-0363
cert-bund: WID-SEC-2022-0271
cert-bund: WID-SEC-2022-0130
cert-bund: WID-SEC-2022-0078
dfn-cert: DFN-CERT-2024-0608
dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-3164
dfn-cert: DFN-CERT-2023-3150
dfn-cert: DFN-CERT-2023-2966
dfn-cert: DFN-CERT-2023-2965
dfn-cert: DFN-CERT-2023-2946
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2675
dfn-cert: DFN-CERT-2022-2565
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-1718
dfn-cert: DFN-CERT-2022-1572
dfn-cert: DFN-CERT-2022-1526
dfn-cert: DFN-CERT-2022-1421
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-1355
dfn-cert: DFN-CERT-2022-1257
dfn-cert: DFN-CERT-2022-1237
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6452-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6452-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.20
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.20
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.20
```

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 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Vim could be made to divide by zero. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04. (CVE-2023-3896)
It was discovered that Vim did not properly manage memory. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-4733, CVE-2023-4750)
It was discovered that Vim contained an arithmetic overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-4734)
It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-4735, CVE-2023-5344)
It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-4738)
It was discovered that Vim could be made to write out of bounds. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-4751)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim did not properly manage memory. 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, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-4752, CVE-2023-5535)
It was discovered that Vim could be made to write out of bounds. 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, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-4781)
It was discovered that Vim could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-5441)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6452-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6452.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6452-1`
`cve: CVE-2023-3896`
`cve: CVE-2023-4733`
`cve: CVE-2023-4734`
`cve: CVE-2023-4735`
`cve: CVE-2023-4738`
`cve: CVE-2023-4750`
`cve: CVE-2023-4751`
`cve: CVE-2023-4752`
`cve: CVE-2023-4781`
`cve: CVE-2023-5344`
`cve: CVE-2023-5441`
`cve: CVE-2023-5535`
`advisory_id: USN-6452-1`
`cert-bund: WID-SEC-2023-3094`
`cert-bund: WID-SEC-2023-2753`
`cert-bund: WID-SEC-2023-2633`
`cert-bund: WID-SEC-2023-2581`
`cert-bund: WID-SEC-2023-2542`
`cert-bund: WID-SEC-2023-2269`
`cert-bund: WID-SEC-2023-2260`
`cert-bund: WID-SEC-2023-2249`
`cert-bund: WID-SEC-2023-1974`
`dfn-cert: DFN-CERT-2024-0608`
`dfn-cert: DFN-CERT-2023-3094`
`dfn-cert: DFN-CERT-2023-3093`
`dfn-cert: DFN-CERT-2023-3092`
`dfn-cert: DFN-CERT-2023-2966`
`dfn-cert: DFN-CERT-2023-2965`
`dfn-cert: DFN-CERT-2023-2631`
`dfn-cert: DFN-CERT-2023-2630`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2581
dfn-cert: DFN-CERT-2023-2410
dfn-cert: DFN-CERT-2023-2371
dfn-cert: DFN-CERT-2023-2343
dfn-cert: DFN-CERT-2023-2077

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6302-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6302-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.17
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.17
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.17
```

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

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

Vulnerability Insight
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2522, CVE-2022-2580, CVE-2022-2817, CVE-2022-2819, CVE-2022-2862, CVE-2022-2889, CVE-2022-2982, CVE-2022-3134)
It was discovered that Vim did not properly perform bounds checks in the diff mode in certain situations. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2598)
It was discovered that Vim did not properly perform bounds checks in certain situations. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2816)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim incorrectly handled memory when skipping compiled code. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2874)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-3016, CVE-2022-3037)
It was discovered that Vim incorrectly handled memory when invalid line number on ':for' is ignored. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3099)
It was discovered that Vim incorrectly handled memory when passing invalid arguments to the assert_fails() method. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3153)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6302-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6302.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6302-1`
`cve: CVE-2022-2522`
`cve: CVE-2022-2580`
`cve: CVE-2022-2598`
`cve: CVE-2022-2816`
`cve: CVE-2022-2817`
`cve: CVE-2022-2819`
`cve: CVE-2022-2862`
`cve: CVE-2022-2874`
`cve: CVE-2022-2889`
`cve: CVE-2022-2982`
`cve: CVE-2022-3016`
`cve: CVE-2022-3037`
`cve: CVE-2022-3099`
`cve: CVE-2022-3134`
`cve: CVE-2022-3153`
`advisory_id: USN-6302-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2022-1372`
`cert-bund: WID-SEC-2022-1324`
`cert-bund: WID-SEC-2022-1284`
`cert-bund: WID-SEC-2022-1223`
`cert-bund: WID-SEC-2022-1195`
`cert-bund: WID-SEC-2022-1085`
`cert-bund: WID-SEC-2022-1076`
`cert-bund: WID-SEC-2022-1073`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1059
cert-bund: WID-SEC-2022-1048
cert-bund: WID-SEC-2022-0880
cert-bund: WID-SEC-2022-0827
dfn-cert: DFN-CERT-2023-1934
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2819
dfn-cert: DFN-CERT-2022-2716
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-1995
dfn-cert: DFN-CERT-2022-1993
dfn-cert: DFN-CERT-2022-1936
dfn-cert: DFN-CERT-2022-1887
dfn-cert: DFN-CERT-2022-1826

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6270-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6270-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.16
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.16
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.16
```

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.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2182)
It was discovered that Vim incorrectly handled memory when deleting buffers in diff mode. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2208)
It was discovered that Vim incorrectly handled memory access. An attacker could possibly use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-2210)
It was discovered that Vim incorrectly handled memory when using nested :source. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2231)
It was discovered that Vim did not properly perform bounds checks when processing a menu item with the only modifier. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2257)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possibly execute arbitrary code. (CVE-2022-2264, CVE-2022-2284, CVE-2022-2289)
It was discovered that Vim did not properly perform bounds checks when going over the end of the typahead. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2285)
It was discovered that Vim did not properly perform bounds checks when reading the provided string. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2286)
It was discovered that Vim incorrectly handled memory when adding words with a control character to the internal spell word list. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2287)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6270-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6270.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6270-1`
`cve: CVE-2022-2182`
`cve: CVE-2022-2208`
`cve: CVE-2022-2210`
`cve: CVE-2022-2231`
`cve: CVE-2022-2257`
`cve: CVE-2022-2264`
`cve: CVE-2022-2284`
`cve: CVE-2022-2285`
`cve: CVE-2022-2286`
`cve: CVE-2022-2287`
`cve: CVE-2022-2289`

... continues on next page ...

... continued from previous page ...

```
advisory_id: USN-6270-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0563
cert-bund: WID-SEC-2022-0548
cert-bund: WID-SEC-2022-0509
cert-bund: WID-SEC-2022-0485
cert-bund: WID-SEC-2022-0459
dfn-cert: DFN-CERT-2023-1787
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-1995
dfn-cert: DFN-CERT-2022-1572
dfn-cert: DFN-CERT-2022-1544
dfn-cert: DFN-CERT-2022-1443
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6313-1)

Summary
The remote host is missing an update for the 'faad2' package(s) announced via the USN-6313-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libfaad2
Installed version:    libfaad2-2.9.1-1
Fixed version:      >=libfaad2-2.9.1-1ubuntu0.1
```

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

Affected Software/OS
'faad2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that FAAD2 incorrectly handled certain inputs. 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 execute arbitrary code. (CVE-2021-32272, CVE-2021-32273, CVE-2021-32274, CVE-2021-32277, CVE-2021-32278, CVE-2023-38857, CVE-2023-38858)
It was discovered that FAAD2 incorrectly handled certain inputs. 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. (CVE-2021-32276)

... 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-6313-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6313.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6313-1`
`cve: CVE-2021-32272`
`cve: CVE-2021-32273`
`cve: CVE-2021-32274`
`cve: CVE-2021-32276`
`cve: CVE-2021-32277`
`cve: CVE-2021-32278`
`cve: CVE-2023-38857`
`cve: CVE-2023-38858`
`advisory_id: USN-6313-1`
`dfn-cert: DFN-CERT-2023-2003`
`dfn-cert: DFN-CERT-2022-0693`
`dfn-cert: DFN-CERT-2021-2226`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6154-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-6154-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.15
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.15
```

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

Affected Software/OS

... continues on next page ...

. . . continued from previous page . . .

'vim' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Vim was using uninitialized memory when fuzzy matching, which could lead to invalid memory access. 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, Ubuntu 22.10 and Ubuntu 23.04. (CVE-2023-2426)
It was discovered that Vim was not properly performing bounds checks when processing register contents, which could lead to a NULL pointer dereference. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-2609)
It was discovered that Vim was not properly limiting the length of substitution expression strings, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-2610)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6154-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6154.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6154-1`
`cve: CVE-2023-2426`
`cve: CVE-2023-2609`
`cve: CVE-2023-2610`
`advisory_id: USN-6154-1`
`cert-bund: WID-SEC-2023-1170`
`cert-bund: WID-SEC-2023-1108`
`dfn-cert: DFN-CERT-2024-0174`
`dfn-cert: DFN-CERT-2023-2000`
`dfn-cert: DFN-CERT-2023-1347`
`dfn-cert: DFN-CERT-2023-1159`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6360-1)

Summary
The remote host is missing an update for the 'flac' package(s) announced via the USN-6360-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  libflac8`
`Installed version:  libflac8-1.3.3-1build1`

. . . continues on next page . . .

... continued from previous page ...

Fixed version: >=libflac8-1.3.3-1ubuntu0.2

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

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

Vulnerability Insight
It was discovered that FLAC incorrectly handled encoding certain files. A remote attacker could use this issue to cause FLAC to crash, resulting in 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-6360-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6360.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6360-1
cve: CVE-2020-22219
advisory_id: USN-6360-1
cert-bund: WID-SEC-2023-2306
dfn-cert: DFN-CERT-2023-2041

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6485-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-6485-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: intel-microcode
Installed version: intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version: >=intel-microcode-3.20231114.0ubuntu0.20.04.1

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'intel-microcode' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Benoit Morgan, Paul Grosen, Thais Moreira Hamasaki, Ke Sun, Alyssa Milburn, Hisham Shafi, Nir Shlomovich, Tavis Ormandy, Daniel Moghimi, Josh Eads, Salman Qazi, Alexandra Sandulescu, Andy Nguyen, Eduardo Vela, Doug Kwan, and Kostik Shtoyk discovered that some Intel(R) Processors did not properly handle certain sequences of processor instructions. A local attacker could possibly use this to cause a core hang (resulting in a denial of service), gain access to sensitive information or possibly escalate their privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6485-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6485.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6485-1`
`cve: CVE-2023-23583`
`advisory_id: USN-6485-1`
`cert-bund: WID-SEC-2023-2906`
`dfn-cert: DFN-CERT-2023-2852`
`dfn-cert: DFN-CERT-2023-2821`
`dfn-cert: DFN-CERT-2023-2621`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6101-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-6101-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   binutils
Installed version:    binutils-2.34-6ubuntu1.1
Fixed version:      >=binutils-2.34-6ubuntu1.5
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'binutils' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that GNU binutils incorrectly handled certain DWARF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 22.10. (CVE-2023-1579)
It was discovered that GNU binutils did not properly verify the version definitions in zer0-lengthverdef table. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 22.04 LTS, Ubuntu 22.10 and Ubuntu 23.04. (CVE-2023-1972)
It was discovered that GNU binutils did not properly validate the size of length parameter in vms-alpha. An attacker could possibly use this issue to cause a crash or access sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2023-25584)
It was discovered that GNU binutils did not properly initialized the file_table field of struct module and the_bfd field of asymbol. An attacker could possibly use this issue to cause a crash. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-25585, CVE-2023-25588)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6101-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6101.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6101-1`
`cve: CVE-2023-1579`
`cve: CVE-2023-1972`
`cve: CVE-2023-25584`
`cve: CVE-2023-25585`
`cve: CVE-2023-25588`
`advisory_id: USN-6101-1`
`cert-bund: WID-SEC-2023-2369`
`cert-bund: WID-SEC-2023-0900`
`cert-bund: WID-SEC-2023-0728`
`dfn-cert: DFN-CERT-2024-1274`
`dfn-cert: DFN-CERT-2024-1163`
`dfn-cert: DFN-CERT-2023-2222`
`dfn-cert: DFN-CERT-2023-1199`
`dfn-cert: DFN-CERT-2023-0844`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5149-1)

Summary
The remote host is missing an update for the 'accountsservice' package(s) announced via the USN-5149-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   accountsservice
Installed version:    accountsservice-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=accountsservice-0.6.55-0ubuntu12~20.04.5
Vulnerable package:   libaccountsservice0
Installed version:    libaccountsservice0-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=libaccountsservice0-0.6.55-0ubuntu12~20.04.5
```

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

Affected Software/OS
'accountsservice' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Kevin Backhouse discovered that AccountsService incorrectly handled memory when performing certain language setting operations. A local attacker could use this issue to escalate privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5149-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5149.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5149-1
cve: CVE-2021-3939
advisory_id: USN-5149-1
dfn-cert: DFN-CERT-2021-2426
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6190-1)

Summary
The remote host is missing an update for the 'accountsservice' package(s) announced via the USN-6190-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   accountsservice
Installed version:    accountsservice-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=accountsservice-0.6.55-0ubuntu12~20.04.6
Vulnerable package:   libaccountsservice0
Installed version:    libaccountsservice0-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=libaccountsservice0-0.6.55-0ubuntu12~20.04.6
```

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

Affected Software/OS
'accountsservice' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Kevin Backhouse discovered that AccountsService incorrectly handled certain D-Bus messages. A local attacker could use this issue to cause AccountsService to crash, resulting in 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-6190-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6190.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6190-1
cve: CVE-2023-3297
advisory_id: USN-6190-1
dfn-cert: DFN-CERT-2023-1494
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6407-1)

Summary
The remote host is missing an update for the 'libx11' package(s) announced via the USN-6407-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libx11-6
Installed version:    libx11-6-2:1.6.9-2ubuntu1.2
Fixed version:      >=libx11-6-2:1.6.9-2ubuntu1.6
```

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

Affected Software/OS
'libx11' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Gregory James Duck discovered that libx11 incorrectly handled certain keyboard symbols. If a user were tricked into connecting to a malicious X server, a remote attacker could use this issue to cause libx11 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-43785)
Yair Mizrahi discovered that libx11 incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to consume memory, leading to a denial of service. (CVE-2023-43786)
Yair Mizrahi discovered that libx11 incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could use this issue to cause libx11 to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-43787)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6407-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6407.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6407-1
cve: CVE-2023-43785
cve: CVE-2023-43786
cve: CVE-2023-43787
advisory_id: USN-6407-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2023-2544
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2375
dfn-cert: DFN-CERT-2023-2361
dfn-cert: DFN-CERT-2023-2360
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5760-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-5760-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version:      >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.5
```

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash. (CVE-2022-2309)
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to expose sensitive information or cause a crash. (CVE-2022-40303)
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-40304)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5760-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5760.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5760-1
cve: CVE-2022-2309
cve: CVE-2022-40303
cve: CVE-2022-40304
advisory_id: USN-5760-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0633
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-2321
cert-bund: WID-SEC-2022-2313
cert-bund: WID-SEC-2022-1787
cert-bund: WID-SEC-2022-0864
dfn-cert: DFN-CERT-2024-0232
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1022
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2023-0105
dfn-cert: DFN-CERT-2022-2842
dfn-cert: DFN-CERT-2022-2841
dfn-cert: DFN-CERT-2022-2838
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2753
dfn-cert: DFN-CERT-2022-2538
dfn-cert: DFN-CERT-2022-2537
dfn-cert: DFN-CERT-2022-2421
dfn-cert: DFN-CERT-2022-2378
dfn-cert: DFN-CERT-2022-2352
dfn-cert: DFN-CERT-2022-1869
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6408-1)

Summary
The remote host is missing an update for the 'libxpm' package(s) announced via the USN-6408-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libxpm4
Installed version:    libxpm4-1:3.5.12-1
Fixed version:      >=libxpm4-1:3.5.12-1ubuntu0.20.04.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libxpm' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Yair Mizrahi discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to consume memory, leading to a denial of service. (CVE-2023-43786)
Yair Mizrahi discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could use this issue to cause libXpm to crash, leading to a denial of service, or possibly execute arbitrary code. (CVE-2023-43787)
Alan Coopersmith discovered that libXpm incorrectly handled certain malformed XPM image files. If a user were tricked into opening a specially crafted XPM image file, a remote attacker could possibly use this issue to cause libXpm to crash, leading to a denial of service. (CVE-2023-43788, CVE-2023-43789)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6408-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6408.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6408-1`
`cve: CVE-2023-43786`
`cve: CVE-2023-43787`
`cve: CVE-2023-43788`
`cve: CVE-2023-43789`
`advisory_id: USN-6408-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2023-2544`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2023-2488`
`dfn-cert: DFN-CERT-2023-2381`
`dfn-cert: DFN-CERT-2023-2375`
`dfn-cert: DFN-CERT-2023-2361`
`dfn-cert: DFN-CERT-2023-2360`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5017-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5017-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.80.84
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the virtual file system implementation in the Linux kernel contained an unsigned to signed integer conversion error. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-33909)
It was discovered that the bluetooth subsystem in the Linux kernel did not properly perform access control. An authenticated attacker could possibly use this to expose sensitive information. (CVE-2020-26558, CVE-2021-0129)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5017-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5017.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5017-1
cve: CVE-2020-26558
cve: CVE-2021-0129
cve: CVE-2021-33909
advisory_id: USN-5017-1
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-2047
cert-bund: WID-SEC-2022-1813
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-0965
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-0624
cert-bund: CB-K21/1268
cert-bund: CB-K21/1251
cert-bund: CB-K21/0775
cert-bund: CB-K21/0615
cert-bund: CB-K21/0568
dfn-cert: DFN-CERT-2022-2356
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2021-2540
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2434
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2355
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1802
dfn-cert: DFN-CERT-2021-1796
dfn-cert: DFN-CERT-2021-1767
dfn-cert: DFN-CERT-2021-1744
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1722
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1692
dfn-cert: DFN-CERT-2021-1678
dfn-cert: DFN-CERT-2021-1653
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1617
dfn-cert: DFN-CERT-2021-1608
dfn-cert: DFN-CERT-2021-1607
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1571
dfn-cert: DFN-CERT-2021-1565
dfn-cert: DFN-CERT-2021-1564
dfn-cert: DFN-CERT-2021-1563
dfn-cert: DFN-CERT-2021-1562
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1559
dfn-cert: DFN-CERT-2021-1558
dfn-cert: DFN-CERT-2021-1556
dfn-cert: DFN-CERT-2021-1555
dfn-cert: DFN-CERT-2021-1554
dfn-cert: DFN-CERT-2021-1553
dfn-cert: DFN-CERT-2021-1552
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1535
dfn-cert: DFN-CERT-2021-1531
dfn-cert: DFN-CERT-2021-1530
dfn-cert: DFN-CERT-2021-1506
dfn-cert: DFN-CERT-2021-1480
dfn-cert: DFN-CERT-2021-1397
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1353
dfn-cert: DFN-CERT-2021-1306
dfn-cert: DFN-CERT-2021-1252
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-1156

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5093-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5093-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vim
Installed version: vim-2:8.1.2269-1ubuntu5
Fixed version: >=vim-2:8.1.2269-1ubuntu5.3

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 21.04.

Vulnerability Insight
Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-3770)
Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3778)

... continues on next page ...

... continued from previous page ...

Dhiraj Mishra discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. (CVE-2021-3796)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5093-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5093.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5093-1`
`cve: CVE-2021-3770`
`cve: CVE-2021-3778`
`cve: CVE-2021-3796`
`advisory_id: USN-5093-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-1120`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0343`
`cert-bund: WID-SEC-2022-0342`
`cert-bund: WID-SEC-2022-0302`
`dfn-cert: DFN-CERT-2022-2921`
`dfn-cert: DFN-CERT-2022-1367`
`dfn-cert: DFN-CERT-2022-0503`
`dfn-cert: DFN-CERT-2022-0369`
`dfn-cert: DFN-CERT-2022-0038`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2370`
`dfn-cert: DFN-CERT-2021-2174`
`dfn-cert: DFN-CERT-2021-2027`
`dfn-cert: DFN-CERT-2021-1872`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5091-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5091-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.88.92
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack. An attacker could use this to expose sensitive information. (CVE-2021-33624)
It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. (CVE-2021-3679)
Alexey Kardashevskiy discovered that the KVM implementation for PowerPC systems in the Linux kernel did not properly validate RTAS arguments in some situations. An attacker in a guest vm could use this to cause a denial of service (host OS crash) or possibly execute arbitrary code. (CVE-2021-37576)
It was discovered that the Virtio console implementation in the Linux kernel did not properly validate input lengths in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2021-38160)
Michael Wakabayashi discovered that the NFSv4 client implementation in the Linux kernel did not properly order connection setup operations. An attacker controlling a remote NFS server could use this to cause a denial of service on the client. (CVE-2021-38199)
It was discovered that the MAX-3421 host USB device driver in the Linux kernel did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2021-38204)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5091-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5091.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5091-1`
`cve: CVE-2021-33624`
`cve: CVE-2021-3679`
`cve: CVE-2021-37576`

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-38160
cve: CVE-2021-38199
cve: CVE-2021-38204
advisory_id: USN-5091-1
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0316
cert-bund: WID-SEC-2022-0137
cert-bund: WID-SEC-2022-0112
cert-bund: CB-K22/0686
cert-bund: CB-K22/0274
cert-bund: CB-K21/1251
cert-bund: CB-K21/0841
cert-bund: CB-K21/0838
cert-bund: CB-K21/0808
cert-bund: CB-K21/0679
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0512
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2540
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2321
dfn-cert: DFN-CERT-2021-2244
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2211
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-2157
dfn-cert: DFN-CERT-2021-2156
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2145
dfn-cert: DFN-CERT-2021-2144
dfn-cert: DFN-CERT-2021-2135
dfn-cert: DFN-CERT-2021-2134
dfn-cert: DFN-CERT-2021-2133

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2092
dfn-cert: DFN-CERT-2021-2071
dfn-cert: DFN-CERT-2021-2032
dfn-cert: DFN-CERT-2021-2030
dfn-cert: DFN-CERT-2021-2023
dfn-cert: DFN-CERT-2021-2022
dfn-cert: DFN-CERT-2021-2011
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1993
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1986
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1938
dfn-cert: DFN-CERT-2021-1898
dfn-cert: DFN-CERT-2021-1885
dfn-cert: DFN-CERT-2021-1879
dfn-cert: DFN-CERT-2021-1878
dfn-cert: DFN-CERT-2021-1815
dfn-cert: DFN-CERT-2021-1763
dfn-cert: DFN-CERT-2021-1744
dfn-cert: DFN-CERT-2021-1707
dfn-cert: DFN-CERT-2021-1699
dfn-cert: DFN-CERT-2021-1698
dfn-cert: DFN-CERT-2021-1697
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1621
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1506
dfn-cert: DFN-CERT-2021-1491
dfn-cert: DFN-CERT-2021-1480
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5116-1)

Summary
The remote host is missing an update for the 'linux, linux-bluefield, linux-gcp-5.4, linux-hwe-5.4, linux-kvm' package(s) announced via the USN-5116-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package: linux-image-generic`

... continues on next page ...

... continued from previous page ...

```
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.89.93
```

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

Affected Software/OS
'linux, linux-bluefield, linux-gcp-5.4, linux-hwe-5.4, linux-kvm' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that a race condition existed in the Atheros Ath9k WiFi driver in the Linux kernel. An attacker could possibly use this to expose sensitive information (WiFi network traffic). (CVE-2020-3702)
Alois Wohlschlager discovered that the overlay file system in the Linux kernel did not restrict private clones in some situations. An attacker could use this to expose sensitive information. (CVE-2021-3732)
It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly compute the access permissions for shadow pages in some situations. A local attacker could use this to cause a denial of service. (CVE-2021-38198)
It was discovered that the Xilinx 10/100 Ethernet Lite device driver in the Linux kernel could report pointer addresses in some situations. An attacker could use this information to ease the exploitation of another vulnerability. (CVE-2021-38205)
It was discovered that the ext4 file system in the Linux kernel contained a race condition when writing xattrs to an inode. A local attacker could use this to cause a denial of service or possibly gain administrative privileges. (CVE-2021-40490)
It was discovered that the 6pack network protocol driver in the Linux kernel did not properly perform validation checks. A privileged attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-42008)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5116-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5116.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5116-1`
`cve: CVE-2020-3702`
`cve: CVE-2021-3732`
`cve: CVE-2021-38198`
`cve: CVE-2021-38205`
`cve: CVE-2021-40490`
`cve: CVE-2021-42008`
`advisory_id: USN-5116-1`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-0876
cert-bund: WID-SEC-2022-2063
cert-bund: WID-SEC-2022-0316
cert-bund: CB-K22/0005
cert-bund: CB-K21/1249
cert-bund: CB-K21/1031
cert-bund: CB-K21/0937
cert-bund: CB-K21/0841
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2022-0737
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0237
dfn-cert: DFN-CERT-2022-0014
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2545
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2212
dfn-cert: DFN-CERT-2021-2211
dfn-cert: DFN-CERT-2021-2210
dfn-cert: DFN-CERT-2021-2183
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2137
dfn-cert: DFN-CERT-2021-2120
dfn-cert: DFN-CERT-2021-2106
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2032
dfn-cert: DFN-CERT-2021-2030
dfn-cert: DFN-CERT-2021-2023
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2011
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1999
dfn-cert: DFN-CERT-2021-1993
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1986
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1949
dfn-cert: DFN-CERT-2021-1938
dfn-cert: DFN-CERT-2021-1907
dfn-cert: DFN-CERT-2021-1895
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5137-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm' package(s) announced via the USN-5137-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.90.94
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the f2fs file system in the Linux kernel did not properly validate metadata in some situations. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2019-19449)

... continues on next page ...

... continued from previous page ...

It was discovered that the Infiniband RDMA userspace connection manager implementation in the Linux kernel contained a race condition leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possible execute arbitrary code. (CVE-2020-36385)
Wolfgang Frisch discovered that the ext4 file system implementation in the Linux kernel contained an integer overflow when handling metadata inode extents. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2021-3428)
Benedict Schlueter discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side- channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-34556)
Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass (SSB) side-channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2021-35477)
It was discovered that the btrfs file system in the Linux kernel did not properly handle removing a non-existent device id. An attacker with CAP_SYS_ADMIN could use this to cause a denial of service. (CVE-2021-3739)
It was discovered that the Qualcomm IPC Router protocol implementation in the Linux kernel did not properly validate metadata in some situations. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2021-3743)
It was discovered that the virtual terminal (vt) device implementation in the Linux kernel contained a race condition in its ioctl handling that led to an out-of-bounds read vulnerability. A local attacker could possibly use this to expose sensitive information. (CVE-2021-3753)
It was discovered that the Linux kernel did not properly account for the memory usage of certain IPC objects. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3759)
It was discovered that the Aspeed Low Pin Count (LPC) Bus Controller implementation in the Linux kernel did not properly perform boundary checks in some situations, allowing out-of-bounds write access. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. In Ubuntu, this issue only affected systems running armhf kernels. (CVE-2021-42252)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5137-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5137.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5137-1`
`cve: CVE-2019-19449`
`cve: CVE-2020-36385`
`cve: CVE-2021-3428`
`cve: CVE-2021-34556`
`cve: CVE-2021-35477`
`cve: CVE-2021-3739`
`cve: CVE-2021-3743`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2021-3753
cve: CVE-2021-3759
cve: CVE-2021-42252
advisory_id: USN-5137-1
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-0879
cert-bund: WID-SEC-2022-2097
cert-bund: WID-SEC-2022-2064
cert-bund: WID-SEC-2022-1895
cert-bund: WID-SEC-2022-1470
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0219
cert-bund: WID-SEC-2022-0217
cert-bund: WID-SEC-2022-0137
cert-bund: CB-K22/0686
cert-bund: CB-K21/1054
cert-bund: CB-K21/0984
cert-bund: CB-K21/0929
cert-bund: CB-K21/0919
cert-bund: CB-K21/0914
cert-bund: CB-K21/0821
cert-bund: CB-K21/0621
cert-bund: CB-K21/0285
cert-bund: CB-K20/0051
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-1595
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2022-2905
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0103
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2563
dfn-cert: DFN-CERT-2021-2560
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2497
dfn-cert: DFN-CERT-2021-2490
dfn-cert: DFN-CERT-2021-2489
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2422
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2386
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2322
dfn-cert: DFN-CERT-2021-2321
dfn-cert: DFN-CERT-2021-2320
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2312
dfn-cert: DFN-CERT-2021-2280
dfn-cert: DFN-CERT-2021-2244
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2213
dfn-cert: DFN-CERT-2021-2211
dfn-cert: DFN-CERT-2021-2183
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2106
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2032
dfn-cert: DFN-CERT-2021-2023
dfn-cert: DFN-CERT-2021-2011
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1992
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1938
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1683
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1617
dfn-cert: DFN-CERT-2021-1574

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1480
dfn-cert: DFN-CERT-2021-1397
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1200
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-0991
dfn-cert: DFN-CERT-2021-0789
dfn-cert: DFN-CERT-2021-0785
dfn-cert: DFN-CERT-2021-0784
dfn-cert: DFN-CERT-2021-0759
dfn-cert: DFN-CERT-2021-0758
dfn-cert: DFN-CERT-2021-0731
dfn-cert: DFN-CERT-2021-0655
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5210-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5210-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.92.96
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. (CVE-2021-4002)
It was discovered that the Linux kernel did not properly enforce certain types of entries in the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. An attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2020-26541)
It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-20321)
It was discovered that the NFC subsystem in the Linux kernel contained a use-after-free vulnerability in its NFC Controller Interface (NCI) implementation. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-3760)
It was discovered that an integer overflow could be triggered in the eBPF implementation in the Linux kernel when preallocating objects for stack maps. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-41864)
It was discovered that the KVM implementation for POWER8 processors in the Linux kernel did not properly keep track if a wakeup event could be resolved by a guest. An attacker in a guest VM could possibly use this to cause a denial of service (host OS crash). (CVE-2021-43056)
It was discovered that the ISDN CAPI implementation in the Linux kernel contained a race condition in certain situations that could trigger an array out-of-bounds bug. A privileged local attacker could possibly use this to cause a denial of service or execute arbitrary code. (CVE-2021-43389)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5210-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5210.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5210-1`
`cve: CVE-2020-26541`
`cve: CVE-2021-20321`
`cve: CVE-2021-3760`
`cve: CVE-2021-4002`
`cve: CVE-2021-41864`
`cve: CVE-2021-43056`
`cve: CVE-2021-43389`
`advisory_id: USN-5210-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-0598`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0340`
`cert-bund: WID-SEC-2022-0317`
`cert-bund: WID-SEC-2022-0230`
`cert-bund: WID-SEC-2022-0228`
`cert-bund: WID-SEC-2022-0226`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0224
cert-bund: WID-SEC-2022-0137
cert-bund: WID-SEC-2022-0112
cert-bund: CB-K22/0686
cert-bund: CB-K22/0274
cert-bund: CB-K21/1302
cert-bund: CB-K21/1238
cert-bund: CB-K21/1190
cert-bund: CB-K21/1158
cert-bund: CB-K21/1112
cert-bund: CB-K21/1024
cert-bund: CB-K20/1088
dfn-cert: DFN-CERT-2023-1595
dfn-cert: DFN-CERT-2022-2890
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1592
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1420
dfn-cert: DFN-CERT-2022-1419
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1110
dfn-cert: DFN-CERT-2022-1092
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0512
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0196

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0193
dfn-cert: DFN-CERT-2022-0092
dfn-cert: DFN-CERT-2022-0090
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2022-0042
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2022-0023
dfn-cert: DFN-CERT-2022-0022
dfn-cert: DFN-CERT-2022-0021
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2022-0019
dfn-cert: DFN-CERT-2021-2664
dfn-cert: DFN-CERT-2021-2657
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2568
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2538
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2480
dfn-cert: DFN-CERT-2021-2472
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2440
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2385
dfn-cert: DFN-CERT-2021-2384
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2259
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2103
dfn-cert: DFN-CERT-2021-2092
dfn-cert: DFN-CERT-2021-1895
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1406
dfn-cert: DFN-CERT-2020-2476
dfn-cert: DFN-CERT-2020-2450

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5210-2)

Summary
The remote host is missing an update for the 'linux, linux-gcp, linux-gcp-5.4, linux-hwe-5.4' package(s) announced via the USN-5210-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.94.98
```

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

Affected Software/OS
'linux, linux-gcp, linux-gcp-5.4, linux-hwe-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
USN-5210-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused failures to boot in environments with AMD Secure Encrypted Virtualization (SEV) enabled. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. (CVE-2021-4002)
It was discovered that the Linux kernel did not properly enforce certain types of entries in the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. An attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2020-26541)
It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2021-20321)
It was discovered that the NFC subsystem in the Linux kernel contained a use-after-free vulnerability in its NFC Controller Interface (NCI) implementation. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2021-3760)
It was discovered that an integer overflow could be triggered in the eBPF implementation in the Linux kernel when preallocating objects for stack maps. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-41864)
It was discovered that the KVM implementation for POWER8 processors in the Linux kernel did not properly keep track if a wakeup event could be resolved by a guest. An attacker in a guest VM could possibly use this to cause a denial of service (host OS crash). (CVE-2021-43056)

... continues on next page ...

... continued from previous page ...

It was discovered that the ISDN CAPI implementation in the Linux kernel contained a race condition in certain situations that could trigger an array out-of-bounds bug. A privileged local attacker could possibly use this to cause a denial of service or execute arbitrary code. (CVE-2021-43389)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5210-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5210.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5210-2`
`url: https://launchpad.net/bugs/1956575`
`cve: CVE-2020-26541`
`cve: CVE-2021-20321`
`cve: CVE-2021-3760`
`cve: CVE-2021-4002`
`cve: CVE-2021-41864`
`cve: CVE-2021-43056`
`cve: CVE-2021-43389`
`advisory_id: USN-5210-2`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-0598`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0340`
`cert-bund: WID-SEC-2022-0317`
`cert-bund: WID-SEC-2022-0230`
`cert-bund: WID-SEC-2022-0228`
`cert-bund: WID-SEC-2022-0226`
`cert-bund: WID-SEC-2022-0224`
`cert-bund: WID-SEC-2022-0137`
`cert-bund: WID-SEC-2022-0112`
`cert-bund: CB-K22/0686`
`cert-bund: CB-K22/0274`
`cert-bund: CB-K21/1302`
`cert-bund: CB-K21/1238`
`cert-bund: CB-K21/1190`
`cert-bund: CB-K21/1158`
`cert-bund: CB-K21/1112`
`cert-bund: CB-K21/1024`
`cert-bund: CB-K20/1088`
`dfn-cert: DFN-CERT-2023-1595`
`dfn-cert: DFN-CERT-2022-2890`
`dfn-cert: DFN-CERT-2022-1725`
`dfn-cert: DFN-CERT-2022-1592`
`dfn-cert: DFN-CERT-2022-1586`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1420
dfn-cert: DFN-CERT-2022-1419
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1110
dfn-cert: DFN-CERT-2022-1092
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0512
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0193
dfn-cert: DFN-CERT-2022-0092
dfn-cert: DFN-CERT-2022-0090
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2022-0042
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2022-0023
dfn-cert: DFN-CERT-2022-0022
dfn-cert: DFN-CERT-2022-0021
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2022-0019
dfn-cert: DFN-CERT-2021-2664
dfn-cert: DFN-CERT-2021-2657
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2568
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2538
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2480
dfn-cert: DFN-CERT-2021-2472
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2440
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2385
dfn-cert: DFN-CERT-2021-2384
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2259
dfn-cert: DFN-CERT-2021-2221
dfn-cert: DFN-CERT-2021-2103
dfn-cert: DFN-CERT-2021-2092
dfn-cert: DFN-CERT-2021-1895
dfn-cert: DFN-CERT-2021-1560
dfn-cert: DFN-CERT-2021-1406
dfn-cert: DFN-CERT-2020-2476
dfn-cert: DFN-CERT-2020-2450
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5294-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-5294-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.100.104
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'linux' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that the Packet network protocol implementation in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-22600)
Szymon Heidrich discovered that the USB Gadget subsystem in the Linux kernel did not properly restrict the size of control requests for certain gadget types, leading to possible out of bounds reads or writes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-39685)
Jann Horn discovered a race condition in the Unix domain socket implementation in the Linux kernel that could result in a read-after-free. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-4083)
Kirill Tkhai discovered that the XFS file system implementation in the Linux kernel did not calculate size correctly when pre-allocating space in some situations. A local attacker could use this to expose sensitive information. (CVE-2021-4155)
Lin Ma discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel contained a race condition, 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-2021-4202)
Brendan Dolan-Gavitt discovered that the aQuantia AQtion Ethernet device driver in the Linux kernel did not properly validate meta-data coming from the device. A local attacker who can control an emulated device can use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-43975)
Sushma Venkatesh Reddy 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-2022-0330)
It was discovered that the VMware Virtual GPU driver in the Linux kernel did not properly handle certain failure conditions, leading to a stale entry in the file descriptor table. A local attacker could use this to expose sensitive information or possibly gain administrative privileges. (CVE-2022-22942)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5294-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5294.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5294-1`
`cve: CVE-2021-22600`
`cve: CVE-2021-39685`
`cve: CVE-2021-4083`
`cve: CVE-2021-4155`
`cve: CVE-2021-4202`
`cve: CVE-2021-43975`
`cve: CVE-2022-0330`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-22942
advisory_id: USN-5294-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2060
cert-bund: WID-SEC-2022-1319
cert-bund: WID-SEC-2022-1161
cert-bund: WID-SEC-2022-0599
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0322
cert-bund: WID-SEC-2022-0239
cert-bund: WID-SEC-2022-0229
cert-bund: WID-SEC-2022-0112
cert-bund: WID-SEC-2022-0104
cert-bund: WID-SEC-2022-0055
cert-bund: WID-SEC-2022-0053
cert-bund: WID-SEC-2022-0049
cert-bund: CB-K22/0529
cert-bund: CB-K22/0410
cert-bund: CB-K22/0274
cert-bund: CB-K22/0119
cert-bund: CB-K22/0117
cert-bund: CB-K22/0106
cert-bund: CB-K22/0105
cert-bund: CB-K22/0024
cert-bund: CB-K21/1292
cert-bund: CB-K21/1212
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0603
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2038
dfn-cert: DFN-CERT-2022-1962
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1486
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1078
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-1029
dfn-cert: DFN-CERT-2022-1024

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0969
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0901
dfn-cert: DFN-CERT-2022-0887
dfn-cert: DFN-CERT-2022-0876
dfn-cert: DFN-CERT-2022-0839
dfn-cert: DFN-CERT-2022-0824
dfn-cert: DFN-CERT-2022-0823
dfn-cert: DFN-CERT-2022-0803
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0775
dfn-cert: DFN-CERT-2022-0766
dfn-cert: DFN-CERT-2022-0764
dfn-cert: DFN-CERT-2022-0738
dfn-cert: DFN-CERT-2022-0737
dfn-cert: DFN-CERT-2022-0715
dfn-cert: DFN-CERT-2022-0676
dfn-cert: DFN-CERT-2022-0660
dfn-cert: DFN-CERT-2022-0585
dfn-cert: DFN-CERT-2022-0584
dfn-cert: DFN-CERT-2022-0568
dfn-cert: DFN-CERT-2022-0567
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0536
dfn-cert: DFN-CERT-2022-0535
dfn-cert: DFN-CERT-2022-0513
dfn-cert: DFN-CERT-2022-0512
dfn-cert: DFN-CERT-2022-0467
dfn-cert: DFN-CERT-2022-0466
dfn-cert: DFN-CERT-2022-0439
dfn-cert: DFN-CERT-2022-0436
dfn-cert: DFN-CERT-2022-0430
dfn-cert: DFN-CERT-2022-0426
dfn-cert: DFN-CERT-2022-0424
dfn-cert: DFN-CERT-2022-0423
dfn-cert: DFN-CERT-2022-0421
dfn-cert: DFN-CERT-2022-0414
dfn-cert: DFN-CERT-2022-0413
dfn-cert: DFN-CERT-2022-0393
dfn-cert: DFN-CERT-2022-0372
dfn-cert: DFN-CERT-2022-0368
dfn-cert: DFN-CERT-2022-0367
dfn-cert: DFN-CERT-2022-0354
dfn-cert: DFN-CERT-2022-0344

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0342
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0337
dfn-cert: DFN-CERT-2022-0336
dfn-cert: DFN-CERT-2022-0335
dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0318
dfn-cert: DFN-CERT-2022-0261
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0251
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0222
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0193
dfn-cert: DFN-CERT-2022-0186
dfn-cert: DFN-CERT-2022-0162
dfn-cert: DFN-CERT-2022-0141
dfn-cert: DFN-CERT-2022-0127
dfn-cert: DFN-CERT-2022-0092
dfn-cert: DFN-CERT-2022-0090
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2022-0040
dfn-cert: DFN-CERT-2021-2466
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5318-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5318-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.104.108
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

Nick Gregory discovered that the Linux kernel incorrectly handled network offload functionality. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2022-25636)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by ARM to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-23960)

Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by Intel to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information. (CVE-2022-0001, CVE-2022-0002)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5318-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5318.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5318-1`
`url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/BHI`
`cve: CVE-2022-0001`
`cve: CVE-2022-0002`
`cve: CVE-2022-23960`
`cve: CVE-2022-25636`
`advisory_id: USN-5318-1`
`cert-bund: WID-SEC-2023-0018`
`cert-bund: WID-SEC-2022-2234`
`cert-bund: WID-SEC-2022-1406`
`cert-bund: WID-SEC-2022-1319`
`cert-bund: WID-SEC-2022-0767`
`cert-bund: WID-SEC-2022-0237`
`cert-bund: WID-SEC-2022-0236`
`cert-bund: WID-SEC-2022-0003`
`cert-bund: CB-K22/0286`
`cert-bund: CB-K22/0281`
`cert-bund: CB-K22/0218`
`dfn-cert: DFN-CERT-2024-0937`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2023-0021
dfn-cert: DFN-CERT-2022-2756
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2028
dfn-cert: DFN-CERT-2022-1962
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1264
dfn-cert: DFN-CERT-2022-1244
dfn-cert: DFN-CERT-2022-1092
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0936
dfn-cert: DFN-CERT-2022-0921
dfn-cert: DFN-CERT-2022-0892
dfn-cert: DFN-CERT-2022-0876
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0803
dfn-cert: DFN-CERT-2022-0738
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0720
dfn-cert: DFN-CERT-2022-0719
dfn-cert: DFN-CERT-2022-0718
dfn-cert: DFN-CERT-2022-0711
dfn-cert: DFN-CERT-2022-0676
dfn-cert: DFN-CERT-2022-0670
dfn-cert: DFN-CERT-2022-0663
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0550
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0545
dfn-cert: DFN-CERT-2022-0544
dfn-cert: DFN-CERT-2022-0543
dfn-cert: DFN-CERT-2022-0542
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0540
dfn-cert: DFN-CERT-2022-0539
dfn-cert: DFN-CERT-2022-0538
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0534
dfn-cert: DFN-CERT-2022-0533
dfn-cert: DFN-CERT-2022-0532
dfn-cert: DFN-CERT-2022-0530

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0529
dfn-cert: DFN-CERT-2022-0465

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5147-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5147-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vim
Installed version: vim-2:8.1.2269-1ubuntu5
Fixed version: >=vim-2:8.1.2269-1ubuntu5.4

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 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that Vim incorrectly handled permissions on the .swp file. A local attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 14.04 ESM. (CVE-2017-17087)
It was discovered that Vim incorrectly handled restricted mode. A local attacker could possibly use this issue to bypass restricted mode and execute arbitrary commands. Note: This update only makes executing shell commands more difficult. Restricted mode should not be considered a complete security measure. This issue only affected Ubuntu 14.04 ESM. (CVE-2019-20807)
Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possible execute arbitrary code with user privileges. This issue only affected Ubuntu 20.04 LTS, Ubuntu 21.04 and Ubuntu 21.10. (CVE-2021-3872)
It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possible execute arbitrary code with user privileges. (CVE-2021-3903)
It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possible execute arbitrary code with user privileges. (CVE-2021-3927)

... continues on next page ...

... continued from previous page ...

It was discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possible execute arbitrary code with user privileges. (CVE-2021-3928)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5147-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.5147.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5147-1`
`cve: CVE-2017-17087`
`cve: CVE-2019-20807`
`cve: CVE-2021-3872`
`cve: CVE-2021-3903`
`cve: CVE-2021-3927`
`cve: CVE-2021-3928`
`advisory_id: USN-5147-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0347`
`cert-bund: WID-SEC-2022-0346`
`cert-bund: WID-SEC-2022-0345`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K20/0730`
`cert-bund: CB-K20/0597`
`dfn-cert: DFN-CERT-2022-2921`
`dfn-cert: DFN-CERT-2022-2716`
`dfn-cert: DFN-CERT-2022-2517`
`dfn-cert: DFN-CERT-2022-1381`
`dfn-cert: DFN-CERT-2022-1367`
`dfn-cert: DFN-CERT-2022-0572`
`dfn-cert: DFN-CERT-2022-0503`
`dfn-cert: DFN-CERT-2022-0369`
`dfn-cert: DFN-CERT-2022-0248`
`dfn-cert: DFN-CERT-2022-0038`
`dfn-cert: DFN-CERT-2021-2529`
`dfn-cert: DFN-CERT-2021-2416`
`dfn-cert: DFN-CERT-2021-2324`
`dfn-cert: DFN-CERT-2021-2274`
`dfn-cert: DFN-CERT-2021-2174`
`dfn-cert: DFN-CERT-2020-2256`
`dfn-cert: DFN-CERT-2020-1556`
`dfn-cert: DFN-CERT-2020-1192`
`dfn-cert: DFN-CERT-2019-1581`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5358-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-gcp, linux-hwe-5.4, linux-hwe-5.13, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5358-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package: linux-image-generic`
`Installed version: linux-image-generic-5.4.0.77.80`
`Fixed version: >=linux-image-generic-5.4.0.107.111`

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-gcp, linux-hwe-5.4, linux-hwe-5.13, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that the network traffic control implementation 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-2022-1055)
It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-27666)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5358-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5358.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5358-1`
`cve: CVE-2022-1055`
`cve: CVE-2022-27666`
`advisory_id: USN-5358-1`
`cert-bund: WID-SEC-2022-0887`
`cert-bund: WID-SEC-2022-0157`
`cert-bund: WID-SEC-2022-0004`
`cert-bund: CB-K22/0368`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0338
dfn-cert: DFN-CERT-2024-0603
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1778
dfn-cert: DFN-CERT-2022-1689
dfn-cert: DFN-CERT-2022-1638
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1487
dfn-cert: DFN-CERT-2022-1477
dfn-cert: DFN-CERT-2022-1475
dfn-cert: DFN-CERT-2022-1437
dfn-cert: DFN-CERT-2022-1436
dfn-cert: DFN-CERT-2022-1244
dfn-cert: DFN-CERT-2022-1239
dfn-cert: DFN-CERT-2022-1037
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0915
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0840
dfn-cert: DFN-CERT-2022-0839
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0825
dfn-cert: DFN-CERT-2022-0824
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0775
dfn-cert: DFN-CERT-2022-0724
dfn-cert: DFN-CERT-2022-0698

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6196-1)

Summary
The remote host is missing an update for the 'python-reportlab' package(s) announced via the USN-6196-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: python3-reportlab
Installed version: python3-reportlab-3.5.34-1ubuntu1
Fixed version: >=python3-reportlab-3.5.34-1ubuntu1.1

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

Affected Software/OS
'python-reportlab' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that ReportLab incorrectly handled certain PDF files. An attacker could possibly use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6196-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6196.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6196-1
cve: CVE-2023-33733
advisory_id: USN-6196-1
dfn-cert: DFN-CERT-2023-1429

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5247-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5247-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vim
Installed version: vim-2:8.1.2269-1ubuntu5
Fixed version: >=vim-2:8.1.2269-1ubuntu5.6

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'vim' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that vim incorrectly handled parsing of filenames in its search functionality. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service. This issue only affected Ubuntu 21.10. (CVE-2021-3973)
It was discovered that vim incorrectly handled memory when opening and searching the contents of certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2021-3974)
It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. (CVE-2021-3984)
It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges. (CVE-2021-4019)
It was discovered that vim incorrectly handled memory when opening and editing certain files. If a user was tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution with user privileges.(CVE-2021-4069)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5247-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5247.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5247-1`
`cve: CVE-2021-3973`
`cve: CVE-2021-3974`
`cve: CVE-2021-3984`
`cve: CVE-2021-4019`
`cve: CVE-2021-4069`
`advisory_id: USN-5247-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0350`
`cert-bund: WID-SEC-2022-0349`
`cert-bund: WID-SEC-2022-0348`
`cert-bund: WID-SEC-2022-0302`
`dfn-cert: DFN-CERT-2022-2921`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-1174
dfn-cert: DFN-CERT-2022-0572
dfn-cert: DFN-CERT-2022-0503
dfn-cert: DFN-CERT-2022-0369
dfn-cert: DFN-CERT-2022-0248
dfn-cert: DFN-CERT-2022-0205
dfn-cert: DFN-CERT-2021-2552
dfn-cert: DFN-CERT-2021-2529
dfn-cert: DFN-CERT-2021-2521
dfn-cert: DFN-CERT-2021-2457

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5442-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gke, linux-gke-5.4, linux-hwe-5.4, linux-ibm, linux-kvm' package(s) announced via the USN-5442-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.113.117

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gke, linux-gke-5.4, linux-hwe-5.4, linux-ibm, linux-kvm' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Kyle Zeng discovered that the Network Queuing and Scheduling subsystem of the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-29581)
Bing-Jhong Billy Jheng discovered that the io_uring subsystem in the Linux kernel contained in integer overflow. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1116)

... continues on next page ...

... continued from previous page ...

Jann Horn discovered that the Linux kernel did not properly enforce seccomp restrictions in some situations. A local attacker could use this to bypass intended seccomp sandbox restrictions. (CVE-2022-30594)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5442-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5442.1

Version used: `2024-02-01T08:21:47Z`

References

`url: https://ubuntu.com/security/notices/USN-5442-1`
`cve: CVE-2022-1116`
`cve: CVE-2022-29581`
`cve: CVE-2022-30594`
`advisory_id: USN-5442-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-2234`
`cert-bund: WID-SEC-2022-0887`
`cert-bund: WID-SEC-2022-0015`
`cert-bund: WID-SEC-2022-0014`
`cert-bund: WID-SEC-2022-0012`
`cert-bund: CB-K22/0633`
`cert-bund: CB-K22/0626`
`cert-bund: CB-K22/0598`
`dfn-cert: DFN-CERT-2024-0461`
`dfn-cert: DFN-CERT-2024-0249`
`dfn-cert: DFN-CERT-2023-1116`
`dfn-cert: DFN-CERT-2023-0606`
`dfn-cert: DFN-CERT-2023-0167`
`dfn-cert: DFN-CERT-2023-0127`
`dfn-cert: DFN-CERT-2022-2756`
`dfn-cert: DFN-CERT-2022-2569`
`dfn-cert: DFN-CERT-2022-2510`
`dfn-cert: DFN-CERT-2022-2502`
`dfn-cert: DFN-CERT-2022-2468`
`dfn-cert: DFN-CERT-2022-2162`
`dfn-cert: DFN-CERT-2022-2148`
`dfn-cert: DFN-CERT-2022-2135`
`dfn-cert: DFN-CERT-2022-2124`
`dfn-cert: DFN-CERT-2022-2037`
`dfn-cert: DFN-CERT-2022-1953`
`dfn-cert: DFN-CERT-2022-1952`
`dfn-cert: DFN-CERT-2022-1888`
`dfn-cert: DFN-CERT-2022-1867`
`dfn-cert: DFN-CERT-2022-1823`
`dfn-cert: DFN-CERT-2022-1816`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1795
dfn-cert: DFN-CERT-2022-1769
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1689
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1639
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1503
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1484
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1448
dfn-cert: DFN-CERT-2022-1447
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
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-2022-1281
dfn-cert: DFN-CERT-2022-1260
dfn-cert: DFN-CERT-2022-1244
dfn-cert: DFN-CERT-2022-1188
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5467-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5467-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.117.120
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. (CVE-2022-21499)

Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1966)

It was discovered that the SCTP protocol implementation in the Linux kernel did not properly verify VTAGs in some situations. A remote attacker could possibly use this to cause a denial of service (connection disassociation). (CVE-2021-3772)

Eric Biederman discovered that the cgroup process migration implementation in the Linux kernel did not perform permission checks correctly in some situations. A local attacker could possibly use this to gain administrative privileges. (CVE-2021-4197)

Jann Horn discovered that the FUSE file system 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-2022-1011)

Qiuhao Li, Gaoning Pan and Yongkang Jia discovered that the KVM implementation in the Linux kernel did not properly perform guest page table updates in some situations. An attacker in a guest vm could possibly use this to crash the host OS. (CVE-2022-1158)

Duoming Zhou discovered that the 6pack protocol implementation in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-1198)

It was discovered that the PF_KEYv2 implementation in the Linux kernel did not properly initialize kernel memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-1353)

It was discovered that the implementation of X.25 network protocols in the Linux kernel did not terminate link layer sessions properly. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1516)

Demi Marie Obenour and Simon Gaiser discovered that several Xen para- virtualization device frontends did not properly restrict the access rights of device backends. An attacker could possibly use a malicious Xen backend to gain access to memory pages of a guest VM or cause a denial of service in the guest. (CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042)

It was discovered that the USB Gadget file system interface 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 ... [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.

... continues on next page ...

... continued from previous page ...

Details: Ubuntu: Security Advisory (USN-5467-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5467.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5467-1
cve: CVE-2021-3772
cve: CVE-2021-4197
cve: CVE-2022-1011
cve: CVE-2022-1158
cve: CVE-2022-1198
cve: CVE-2022-1353
cve: CVE-2022-1516
cve: CVE-2022-1966
cve: CVE-2022-21499
cve: CVE-2022-23036
cve: CVE-2022-23037
cve: CVE-2022-23038
cve: CVE-2022-23039
cve: CVE-2022-23040
cve: CVE-2022-23041
cve: CVE-2022-23042
cve: CVE-2022-24958
cve: CVE-2022-26966
cve: CVE-2022-28356
cve: CVE-2022-28389
cve: CVE-2022-28390
advisory_id: USN-5467-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2022-2234
cert-bund: WID-SEC-2022-0974
cert-bund: WID-SEC-2022-0887
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0173
cert-bund: WID-SEC-2022-0164
cert-bund: WID-SEC-2022-0163
cert-bund: WID-SEC-2022-0161
cert-bund: WID-SEC-2022-0156
cert-bund: WID-SEC-2022-0155
cert-bund: WID-SEC-2022-0154
cert-bund: WID-SEC-2022-0153
cert-bund: WID-SEC-2022-0149
cert-bund: WID-SEC-2022-0145
cert-bund: WID-SEC-2022-0137
cert-bund: WID-SEC-2022-0018
cert-bund: WID-SEC-2022-0016
cert-bund: CB-K22/0686

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0651
cert-bund: CB-K22/0518
cert-bund: CB-K22/0437
cert-bund: CB-K22/0404
cert-bund: CB-K22/0383
cert-bund: CB-K22/0334
cert-bund: CB-K22/0309
cert-bund: CB-K22/0300
cert-bund: CB-K22/0260
cert-bund: CB-K22/0177
cert-bund: CB-K22/0032
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2023-2018
dfn-cert: DFN-CERT-2023-1848
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2871
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2762
dfn-cert: DFN-CERT-2022-2756
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2382
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2235
dfn-cert: DFN-CERT-2022-2115
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2022-1909
dfn-cert: DFN-CERT-2022-1853
dfn-cert: DFN-CERT-2022-1759
dfn-cert: DFN-CERT-2022-1754
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1689
dfn-cert: DFN-CERT-2022-1677
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1622
dfn-cert: DFN-CERT-2022-1604
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1577
dfn-cert: DFN-CERT-2022-1575

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1510
dfn-cert: DFN-CERT-2022-1504
dfn-cert: DFN-CERT-2022-1503
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1486
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1477
dfn-cert: DFN-CERT-2022-1476
dfn-cert: DFN-CERT-2022-1475
dfn-cert: DFN-CERT-2022-1463
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1448
dfn-cert: DFN-CERT-2022-1447
dfn-cert: DFN-CERT-2022-1445
dfn-cert: DFN-CERT-2022-1439
dfn-cert: DFN-CERT-2022-1437
dfn-cert: DFN-CERT-2022-1436
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1420
dfn-cert: DFN-CERT-2022-1419
dfn-cert: DFN-CERT-2022-1409
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-2022-1359
dfn-cert: DFN-CERT-2022-1347
dfn-cert: DFN-CERT-2022-1346
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1312
dfn-cert: DFN-CERT-2022-1298
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1283
dfn-cert: DFN-CERT-2022-1282
dfn-cert: DFN-CERT-2022-1281
dfn-cert: DFN-CERT-2022-1280
dfn-cert: DFN-CERT-2022-1279
dfn-cert: DFN-CERT-2022-1278
dfn-cert: DFN-CERT-2022-1277
dfn-cert: DFN-CERT-2022-1256
dfn-cert: DFN-CERT-2022-1244
dfn-cert: DFN-CERT-2022-1182
dfn-cert: DFN-CERT-2022-1181

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1110
dfn-cert: DFN-CERT-2022-1092
dfn-cert: DFN-CERT-2022-1082
dfn-cert: DFN-CERT-2022-1074
dfn-cert: DFN-CERT-2022-1073
dfn-cert: DFN-CERT-2022-1072
dfn-cert: DFN-CERT-2022-1071
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-1038
dfn-cert: DFN-CERT-2022-1037
dfn-cert: DFN-CERT-2022-1029
dfn-cert: DFN-CERT-2022-1024
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0915
dfn-cert: DFN-CERT-2022-0893
dfn-cert: DFN-CERT-2022-0881
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0862
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0860
dfn-cert: DFN-CERT-2022-0840
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0803
dfn-cert: DFN-CERT-2022-0795
dfn-cert: DFN-CERT-2022-0790
dfn-cert: DFN-CERT-2022-0775
dfn-cert: DFN-CERT-2022-0766
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0720
dfn-cert: DFN-CERT-2022-0719
dfn-cert: DFN-CERT-2022-0660
dfn-cert: DFN-CERT-2022-0631
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0556
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0439
dfn-cert: DFN-CERT-2022-0379
dfn-cert: DFN-CERT-2022-0344
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0336

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2022-0318
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0251
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0186
dfn-cert: DFN-CERT-2022-0059
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2512
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2313

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5252-1)

Summary
The remote host is missing an update for the 'policykit-1' package(s) announced via the USN-5252-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: policykit-1
Installed version: policykit-1-0.105-26ubuntu1.1
Fixed version: >=policykit-1-0.105-26ubuntu1.2

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

Affected Software/OS
'policykit-1' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that the PolicyKit pkexec tool incorrectly handled command-line arguments. A local attacker could use this issue to escalate privileges to an administrator.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5252-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5252.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5252-1`
`cve: CVE-2021-4034`
`advisory_id: USN-5252-1`
`cert-bund: WID-SEC-2023-0426`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1483`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: CB-K22/0310`
`cert-bund: CB-K22/0098`
`dfn-cert: DFN-CERT-2022-0579`
`dfn-cert: DFN-CERT-2022-0368`
`dfn-cert: DFN-CERT-2022-0320`
`dfn-cert: DFN-CERT-2022-0293`
`dfn-cert: DFN-CERT-2022-0188`
`dfn-cert: DFN-CERT-2022-0110`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5562-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5562-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.124.125
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2588)

It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-2586)

It was discovered that the block layer subsystem in the Linux kernel did not properly initialize memory in some situations. A privileged local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-0494)

Hu Jiahui discovered that multiple race conditions existed in the Advanced Linux Sound Architecture (ALSA) framework, leading to use-after-free vulnerabilities. A local attacker could use these to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1048)

Minh Yuan discovered that the floppy disk driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1652)

It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, 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-2022-1679)

It was discovered that the Marvell NFC device driver implementation in the Linux kernel did not properly perform memory cleanup operations in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1734)

Duoming Zhou discovered a race condition in the NFC subsystem in the Linux kernel, leading to a use-after-free vulnerability. A privileged local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-1974)

Duoming Zhou discovered that the NFC subsystem in the Linux kernel did not properly prevent context switches from occurring during certain atomic context operations. A privileged local attacker could use this to cause a denial of service (system crash). (CVE-2022-1975)

Felix Fu discovered that the Sun RPC implementation in the Linux kernel did not properly handle socket states, leading to 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-2022-28893)

Arthur Mongodin discovered that the netfilter subsystem ... [Please see the references for more information on the vulnerabilities]

... 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-5562-1)

OID:1.3.6.1.4.1.25623.1.1.12.2022.5562.1

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5562-1
cve: CVE-2022-0494
cve: CVE-2022-1048
cve: CVE-2022-1652
cve: CVE-2022-1679
cve: CVE-2022-1734
cve: CVE-2022-1974
cve: CVE-2022-1975
cve: CVE-2022-2586
cve: CVE-2022-2588
cve: CVE-2022-28893
cve: CVE-2022-34918
advisory_id: USN-5562-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-0997
cert-bund: WID-SEC-2022-0560
cert-bund: WID-SEC-2022-0540
cert-bund: WID-SEC-2022-0323
cert-bund: WID-SEC-2022-0251
cert-bund: WID-SEC-2022-0238
cert-bund: WID-SEC-2022-0178
cert-bund: WID-SEC-2022-0135
cert-bund: WID-SEC-2022-0117
cert-bund: CB-K22/0689
cert-bund: CB-K22/0621
cert-bund: CB-K22/0599
cert-bund: CB-K22/0589
cert-bund: CB-K22/0552
cert-bund: CB-K22/0362
cert-bund: CB-K22/0351
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0121
dfn-cert: DFN-CERT-2023-2379
dfn-cert: DFN-CERT-2023-1576
dfn-cert: DFN-CERT-2023-1528
dfn-cert: DFN-CERT-2023-1116

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2649
dfn-cert: DFN-CERT-2022-2623
dfn-cert: DFN-CERT-2022-2621
dfn-cert: DFN-CERT-2022-2620
dfn-cert: DFN-CERT-2022-2619
dfn-cert: DFN-CERT-2022-2618
dfn-cert: DFN-CERT-2022-2617
dfn-cert: DFN-CERT-2022-2616
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2469
dfn-cert: DFN-CERT-2022-2449
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2390
dfn-cert: DFN-CERT-2022-2382
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2274
dfn-cert: DFN-CERT-2022-2254
dfn-cert: DFN-CERT-2022-2172
dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2139
dfn-cert: DFN-CERT-2022-2135
dfn-cert: DFN-CERT-2022-2124
dfn-cert: DFN-CERT-2022-2115
dfn-cert: DFN-CERT-2022-2113
dfn-cert: DFN-CERT-2022-2112
dfn-cert: DFN-CERT-2022-2096
dfn-cert: DFN-CERT-2022-2078
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2067
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-2055
dfn-cert: DFN-CERT-2022-2040
dfn-cert: DFN-CERT-2022-2038

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2037
dfn-cert: DFN-CERT-2022-2034
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2022-1909
dfn-cert: DFN-CERT-2022-1853
dfn-cert: DFN-CERT-2022-1828
dfn-cert: DFN-CERT-2022-1823
dfn-cert: DFN-CERT-2022-1821
dfn-cert: DFN-CERT-2022-1810
dfn-cert: DFN-CERT-2022-1802
dfn-cert: DFN-CERT-2022-1797
dfn-cert: DFN-CERT-2022-1794
dfn-cert: DFN-CERT-2022-1786
dfn-cert: DFN-CERT-2022-1778
dfn-cert: DFN-CERT-2022-1776
dfn-cert: DFN-CERT-2022-1754
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1697
dfn-cert: DFN-CERT-2022-1676
dfn-cert: DFN-CERT-2022-1660
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1598
dfn-cert: DFN-CERT-2022-1592
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1579
dfn-cert: DFN-CERT-2022-1578
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1570
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1564
dfn-cert: DFN-CERT-2022-1557
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1542
dfn-cert: DFN-CERT-2022-1528
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1504
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1486
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1448
dfn-cert: DFN-CERT-2022-1431
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1420
dfn-cert: DFN-CERT-2022-1419
dfn-cert: DFN-CERT-2022-1409

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1347
dfn-cert: DFN-CERT-2022-1346
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-2022-1312
dfn-cert: DFN-CERT-2022-1279
dfn-cert: DFN-CERT-2022-1278
dfn-cert: DFN-CERT-2022-1260
dfn-cert: DFN-CERT-2022-1110
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0893
dfn-cert: DFN-CERT-2022-0881
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0862
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0860
dfn-cert: DFN-CERT-2022-0840
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0701
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5668-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-bluefield, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle' package(s) announced via the USN-5668-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.128.129
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'linux, linux-aws, linux-bluefield, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the BPF verifier in the Linux kernel did not properly handle internal data structures. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-4159)
It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 (V4L2) implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-20369)
Duoming Zhou discovered that race conditions existed in the timer handling implementation of the Linux kernel's Rose X.25 protocol layer, resulting in use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-2318)
Roger Pau Monne discovered that the Xen virtual block driver in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-26365)
Pawan Kumar Gupta, Alyssa Milburn, Amit Peled, Shani Rehana, Nir Shildan and Ariel Sabba discovered that some Intel processors with Enhanced Indirect Branch Restricted Speculation (eIBRS) did not properly handle RET instructions after a VM exits. A local attacker could potentially use this to expose sensitive information. (CVE-2022-26373)
Eric Biggers discovered that a use-after-free vulnerability existed in the io_uring subsystem in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3176)
Roger Pau Monne discovered that the Xen paravirtualization frontend in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information (guest kernel memory). (CVE-2022-33740)
It was discovered that the Xen paravirtualization frontend in the Linux kernel incorrectly shared unrelated data when communicating with certain backends. A local attacker could use this to cause a denial of service (guest crash) or expose sensitive information (guest kernel memory). (CVE-2022-33741, CVE-2022-33742)
Oleksandr Tyshchenko discovered that the Xen paravirtualization platform in the Linux kernel on ARM platforms contained a race condition in certain situations. An attacker in a guest VM could use this to cause a denial of service in the host OS. (CVE-2022-33744)
It was discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a reference counting error. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-36879)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5668-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5668.1
Version used: `2024-02-02T04:09:01Z`

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5668-1
cve: CVE-2021-4159
cve: CVE-2022-20369
cve: CVE-2022-2318
cve: CVE-2022-26365
cve: CVE-2022-26373
cve: CVE-2022-3176
cve: CVE-2022-33740
cve: CVE-2022-33741
cve: CVE-2022-33742
cve: CVE-2022-33744
cve: CVE-2022-36879
advisory_id: USN-5668-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1456
cert-bund: WID-SEC-2022-1207
cert-bund: WID-SEC-2022-0986
cert-bund: WID-SEC-2022-0887
cert-bund: WID-SEC-2022-0841
cert-bund: WID-SEC-2022-0582
cert-bund: WID-SEC-2022-0564
dfn-cert: DFN-CERT-2024-0247
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2482
dfn-cert: DFN-CERT-2023-1595
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0863
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0182
dfn-cert: DFN-CERT-2022-2919
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2818
dfn-cert: DFN-CERT-2022-2817
dfn-cert: DFN-CERT-2022-2632
dfn-cert: DFN-CERT-2022-2608
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2542
dfn-cert: DFN-CERT-2022-2520
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2469
dfn-cert: DFN-CERT-2022-2449
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2338
dfn-cert: DFN-CERT-2022-2334
dfn-cert: DFN-CERT-2022-2326
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2277
dfn-cert: DFN-CERT-2022-2239
dfn-cert: DFN-CERT-2022-2238
dfn-cert: DFN-CERT-2022-2237
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2022-2172
dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2139
dfn-cert: DFN-CERT-2022-2135
dfn-cert: DFN-CERT-2022-2103
dfn-cert: DFN-CERT-2022-2102
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2067
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-2040
dfn-cert: DFN-CERT-2022-2038
dfn-cert: DFN-CERT-2022-2037
dfn-cert: DFN-CERT-2022-2034
dfn-cert: DFN-CERT-2022-1867
dfn-cert: DFN-CERT-2022-1847
dfn-cert: DFN-CERT-2022-1846
dfn-cert: DFN-CERT-2022-1828
dfn-cert: DFN-CERT-2022-1823
dfn-cert: DFN-CERT-2022-1816
dfn-cert: DFN-CERT-2022-1795
dfn-cert: DFN-CERT-2022-1775
dfn-cert: DFN-CERT-2022-1767
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1689
dfn-cert: DFN-CERT-2022-1660
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1592
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1529
dfn-cert: DFN-CERT-2022-1518
dfn-cert: DFN-CERT-2022-1498
dfn-cert: DFN-CERT-2022-0344

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0335

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5613-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5613-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: vim
Installed version: vim-2:8.1.2269-1ubuntu5
Fixed version: >=vim-2:8.1.2269-1ubuntu5.8

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

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

Vulnerability Insight
It was discovered that Vim was not properly performing bounds checks when executing spell suggestion commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0943)
It was discovered that Vim was using freed memory when dealing with regular expressions through its old regular expression engine. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution. (CVE-2022-1154)
It was discovered that Vim was not properly performing checks on name of lambda functions. An attacker could possibly use this issue to cause a denial of service. This issue affected only Ubuntu 22.04 LTS. (CVE-2022-1420)
It was discovered that Vim was incorrectly performing bounds checks when processing invalid commands with composing characters in Ex mode. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1616)
It was discovered that Vim was not properly processing latin1 data when issuing Ex commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1619)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim was not properly performing memory management when dealing with invalid regular expression patterns in buffers. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-1620)
It was discovered that Vim was not properly processing invalid bytes when performing spell check operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1621)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5613-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5613.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5613-1`
`cve: CVE-2022-0943`
`cve: CVE-2022-1154`
`cve: CVE-2022-1420`
`cve: CVE-2022-1616`
`cve: CVE-2022-1619`
`cve: CVE-2022-1620`
`cve: CVE-2022-1621`
`advisory_id: USN-5613-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-1846`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-0767`
`cert-bund: WID-SEC-2022-0171`
`cert-bund: WID-SEC-2022-0126`
`cert-bund: WID-SEC-2022-0124`
`cert-bund: WID-SEC-2022-0115`
`cert-bund: WID-SEC-2022-0032`
`cert-bund: CB-K22/0622`
`dfn-cert: DFN-CERT-2022-2921`
`dfn-cert: DFN-CERT-2022-2675`
`dfn-cert: DFN-CERT-2022-2517`
`dfn-cert: DFN-CERT-2022-2364`
`dfn-cert: DFN-CERT-2022-2051`
`dfn-cert: DFN-CERT-2022-1837`
`dfn-cert: DFN-CERT-2022-1600`
`dfn-cert: DFN-CERT-2022-1474`
`dfn-cert: DFN-CERT-2022-1466`
`dfn-cert: DFN-CERT-2022-1381`
`dfn-cert: DFN-CERT-2022-1367`
`dfn-cert: DFN-CERT-2022-1262`
`dfn-cert: DFN-CERT-2022-1174`
`dfn-cert: DFN-CERT-2022-1118`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1031
dfn-cert: DFN-CERT-2022-0960
dfn-cert: DFN-CERT-2022-0913
dfn-cert: DFN-CERT-2022-0782
dfn-cert: DFN-CERT-2022-0689

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5756-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5756-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.135.133

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-42703)
It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3524)
It was discovered that a race condition existed in the Bluetooth subsystem 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-2022-3564)

... continues on next page ...

... continued from previous page ...

It was discovered that the ISDN implementation of the Linux kernel contained a use-after-free vulnerability. A privileged user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3565)
It was discovered that the TCP implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3566)
It was discovered that the IPv6 implementation in the Linux kernel contained a data race condition. An attacker could possibly use this to cause undesired behaviors. (CVE-2022-3567)
It was discovered that the Realtek RTL8152 USB Ethernet adapter driver in the Linux kernel did not properly handle certain error conditions. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3594)
It was discovered that a null pointer dereference existed in the NILFS2 file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3621)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5756-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5756.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5756-1`
`cve: CVE-2022-3524`
`cve: CVE-2022-3564`
`cve: CVE-2022-3565`
`cve: CVE-2022-3566`
`cve: CVE-2022-3567`
`cve: CVE-2022-3594`
`cve: CVE-2022-3621`
`cve: CVE-2022-42703`
`advisory_id: USN-5756-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2625`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1981`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2023-1669`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2022-1812`
`cert-bund: WID-SEC-2022-1792`
`cert-bund: WID-SEC-2022-1761`
`cert-bund: WID-SEC-2022-1741`
`cert-bund: WID-SEC-2022-1651`
`dfn-cert: DFN-CERT-2024-1398`
`dfn-cert: DFN-CERT-2024-1381`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1848
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1542
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1412
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1371
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1253
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-0749
dfn-cert: DFN-CERT-2023-0726
dfn-cert: DFN-CERT-2023-0656
dfn-cert: DFN-CERT-2023-0583
dfn-cert: DFN-CERT-2023-0573
dfn-cert: DFN-CERT-2023-0572
dfn-cert: DFN-CERT-2023-0508
dfn-cert: DFN-CERT-2023-0500
dfn-cert: DFN-CERT-2023-0483
dfn-cert: DFN-CERT-2023-0467
dfn-cert: DFN-CERT-2023-0460
dfn-cert: DFN-CERT-2023-0459
dfn-cert: DFN-CERT-2023-0378
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0355
dfn-cert: DFN-CERT-2023-0342
dfn-cert: DFN-CERT-2023-0341
dfn-cert: DFN-CERT-2023-0332
dfn-cert: DFN-CERT-2023-0285
dfn-cert: DFN-CERT-2023-0254
dfn-cert: DFN-CERT-2023-0194
dfn-cert: DFN-CERT-2023-0193
dfn-cert: DFN-CERT-2023-0192

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0020
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-2022-2892
dfn-cert: DFN-CERT-2022-2891
dfn-cert: DFN-CERT-2022-2890
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-2022-2835
dfn-cert: DFN-CERT-2022-2833
dfn-cert: DFN-CERT-2022-2818
dfn-cert: DFN-CERT-2022-2817
dfn-cert: DFN-CERT-2022-2787
dfn-cert: DFN-CERT-2022-2737
dfn-cert: DFN-CERT-2022-2736
dfn-cert: DFN-CERT-2022-2735
dfn-cert: DFN-CERT-2022-2733
dfn-cert: DFN-CERT-2022-2732
dfn-cert: DFN-CERT-2022-2713
dfn-cert: DFN-CERT-2022-2712
dfn-cert: DFN-CERT-2022-2649
dfn-cert: DFN-CERT-2022-2646
dfn-cert: DFN-CERT-2022-2632
dfn-cert: DFN-CERT-2022-2623
dfn-cert: DFN-CERT-2022-2621
dfn-cert: DFN-CERT-2022-2620
dfn-cert: DFN-CERT-2022-2619
dfn-cert: DFN-CERT-2022-2618
dfn-cert: DFN-CERT-2022-2617
dfn-cert: DFN-CERT-2022-2616
dfn-cert: DFN-CERT-2022-2609
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-2022-2449

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5791-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5791-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.136.134
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that a race condition existed in the Android Binder IPC subsystem 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-2022-20421)
David Leadbeater discovered that the netfilter IRC protocol tracking implementation in the Linux Kernel incorrectly handled certain message payloads in some situations. A remote attacker could possibly use this to cause a denial of service or bypass firewall filtering. (CVE-2022-2663)
It was discovered that the Intel 740 frame buffer driver in the Linux kernel contained a divide by zero vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3061)
It was discovered that the sound subsystem 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). (CVE-2022-3303)
Gwnaun Jung discovered that the SFB packet scheduling implementation 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-2022-3586)
It was discovered that the NILFS2 file system implementation in the Linux kernel did not properly deallocate memory in certain error conditions. An attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-3646)
Hyunwoo Kim discovered that an integer overflow vulnerability existed in the PXA3xx graphics driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-39842)
It was discovered that a race condition existed in the EFI capsule loader 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-2022-40307)

... continues on next page ...

... continued from previous page ...

Zheng Wang and Zhuorao Yang discovered that the RealTek RTL8712U wireless 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-2022-4095)
It was discovered that the USB monitoring (usbmon) component in the Linux kernel did not properly set permissions on memory mapped in to user space processes. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-43750)
Jann Horn discovered a race condition existed in the Linux kernel when unmapping VMAs in certain situations, resulting in possible use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-39188)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5791-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5791.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5791-1`
`cve: CVE-2022-20421`
`cve: CVE-2022-2663`
`cve: CVE-2022-3061`
`cve: CVE-2022-3303`
`cve: CVE-2022-3586`
`cve: CVE-2022-3646`
`cve: CVE-2022-39188`
`cve: CVE-2022-39842`
`cve: CVE-2022-40307`
`cve: CVE-2022-4095`
`cve: CVE-2022-43750`
`advisory_id: USN-5791-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0773`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2023-0292`
`cert-bund: WID-SEC-2022-2132`
`cert-bund: WID-SEC-2022-1856`
`cert-bund: WID-SEC-2022-1823`
`cert-bund: WID-SEC-2022-1819`
`cert-bund: WID-SEC-2022-1599`
`cert-bund: WID-SEC-2022-1538`
`cert-bund: WID-SEC-2022-1360`
`cert-bund: WID-SEC-2022-1287`
`cert-bund: WID-SEC-2022-1266`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2022-1236
cert-bund: WID-SEC-2022-1218
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2023-2018
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1722
dfn-cert: DFN-CERT-2023-1707
dfn-cert: DFN-CERT-2023-1253
dfn-cert: DFN-CERT-2023-1242
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1091
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1002
dfn-cert: DFN-CERT-2023-0976
dfn-cert: DFN-CERT-2023-0956
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0863
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0332
dfn-cert: DFN-CERT-2023-0269
dfn-cert: DFN-CERT-2023-0020
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-2022-2899
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-2022-2886
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-2022-2787
dfn-cert: DFN-CERT-2022-2737
dfn-cert: DFN-CERT-2022-2713
dfn-cert: DFN-CERT-2022-2712
dfn-cert: DFN-CERT-2022-2646
dfn-cert: DFN-CERT-2022-2632
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-2609
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-2022-2449
dfn-cert: DFN-CERT-2022-2447
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2358
dfn-cert: DFN-CERT-2022-2357
dfn-cert: DFN-CERT-2022-2326
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2291
dfn-cert: DFN-CERT-2022-2275
dfn-cert: DFN-CERT-2022-2274
dfn-cert: DFN-CERT-2022-2273
dfn-cert: DFN-CERT-2022-2172
dfn-cert: DFN-CERT-2022-2171
dfn-cert: DFN-CERT-2022-2162
dfn-cert: DFN-CERT-2022-2148
dfn-cert: DFN-CERT-2022-2139
dfn-cert: DFN-CERT-2022-2138
dfn-cert: DFN-CERT-2022-2135
dfn-cert: DFN-CERT-2022-2124
dfn-cert: DFN-CERT-2022-2069
dfn-cert: DFN-CERT-2022-2067
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-2038
dfn-cert: DFN-CERT-2022-2034
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5613-2)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5613-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.9
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'vim' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-5613-1 fixed vulnerabilities in Vim. Unfortunately that update failed to include binary packages for some architectures. This update fixes that regression.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Vim was not properly performing bounds checks when executing spell suggestion commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-0943)
It was discovered that Vim was using freed memory when dealing with regular expressions through its old regular expression engine. If a user were tricked into opening a specially crafted file, an attacker could crash the application, leading to a denial of service, or possibly achieve code execution. (CVE-2022-1154)
It was discovered that Vim was not properly performing checks on name of lambda functions. An attacker could possibly use this issue to cause a denial of service. This issue affected only Ubuntu 22.04 LTS. (CVE-2022-1420)
It was discovered that Vim was incorrectly performing bounds checks when processing invalid commands with composing characters in Ex mode. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1616)
It was discovered that Vim was not properly processing latin1 data when issuing Ex commands. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1619)
It was discovered that Vim was not properly performing memory management when dealing with invalid regular expression patterns in buffers. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-1620)
It was discovered that Vim was not properly processing invalid bytes when performing spell check operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-1621)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5613-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5613.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5613-2`
`url: https://launchpad.net/bugs/1989973`
`cve: CVE-2022-0943`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-1154
cve: CVE-2022-1420
cve: CVE-2022-1616
cve: CVE-2022-1619
cve: CVE-2022-1620
cve: CVE-2022-1621
advisory_id: USN-5613-2
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0171
cert-bund: WID-SEC-2022-0126
cert-bund: WID-SEC-2022-0124
cert-bund: WID-SEC-2022-0115
cert-bund: WID-SEC-2022-0032
cert-bund: CB-K22/0622
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2675
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-2051
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1474
dfn-cert: DFN-CERT-2022-1466
dfn-cert: DFN-CERT-2022-1381
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-1262
dfn-cert: DFN-CERT-2022-1174
dfn-cert: DFN-CERT-2022-1118
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1076
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-1031
dfn-cert: DFN-CERT-2022-0960
dfn-cert: DFN-CERT-2022-0913
dfn-cert: DFN-CERT-2022-0782
dfn-cert: DFN-CERT-2022-0689

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5801-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5801-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.11
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.11
Vulnerable package:   xxd
Installed version:    xxd-2:8.1.2269-1ubuntu5
Fixed version:      >=xxd-2:8.1.2269-1ubuntu5.11
```

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

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

Vulnerability Insight
It was discovered that Vim makes illegal memory calls when pasting brackets in Ex mode. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. This issue affected only Ubuntu 20.04 and 22.04 (CVE-2022-0392)
It was discovered that Vim makes illegal memory calls when making certain retab calls. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. (CVE-2022-0417)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5801-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5801.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5801-1
cve: CVE-2022-0392
cve: CVE-2022-0417
advisory_id: USN-5801-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0148
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0056
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2675
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-1381
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-0598
dfn-cert: DFN-CERT-2022-0291

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5917-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gke, linux-gkeop, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5917-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.144.142

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gke, linux-gkeop, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

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)
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)
It was discovered that a use-after-free vulnerability existed in the SGI GRU driver in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2022-3424)

... continues on next page ...

... continued from previous page ...

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)
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)
Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-36280)
Hyunwoo Kim discovered that the DVB Core driver in the Linux kernel did not properly perform reference counting in some situations, 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-2022-41218)
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 ... [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-5917-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5917.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5917-1`
`cve: CVE-2022-3169`
`cve: CVE-2022-3424`
`cve: CVE-2022-3435`
`cve: CVE-2022-3521`
`cve: CVE-2022-3545`
`cve: CVE-2022-3623`
`cve: CVE-2022-36280`
`cve: CVE-2022-41218`
`cve: CVE-2022-4139`
`cve: CVE-2022-42328`
`cve: CVE-2022-42329`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-47520
cve: CVE-2022-47929
cve: CVE-2023-0045
cve: CVE-2023-0266
cve: CVE-2023-0394
cve: CVE-2023-0461
cve: CVE-2023-20938
cve: CVE-2023-23454
cve: CVE-2023-23455
advisory_id: USN-5917-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1371
cert-bund: WID-SEC-2023-1101
cert-bund: WID-SEC-2023-0895
cert-bund: WID-SEC-2023-0469
cert-bund: WID-SEC-2023-0292
cert-bund: WID-SEC-2023-0281
cert-bund: WID-SEC-2023-0152
cert-bund: WID-SEC-2023-0112
cert-bund: WID-SEC-2023-0085
cert-bund: WID-SEC-2023-0024
cert-bund: WID-SEC-2022-2361
cert-bund: WID-SEC-2022-2250
cert-bund: WID-SEC-2022-2208
cert-bund: WID-SEC-2022-1812
cert-bund: WID-SEC-2022-1761
cert-bund: WID-SEC-2022-1741
cert-bund: WID-SEC-2022-1648
cert-bund: WID-SEC-2022-1495
cert-bund: WID-SEC-2022-1374
cert-bund: WID-SEC-2022-1361
dfn-cert: DFN-CERT-2024-0841
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0733
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0516
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0452
dfn-cert: DFN-CERT-2024-0333

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0260
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0248
dfn-cert: DFN-CERT-2023-3123
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2543
dfn-cert: DFN-CERT-2023-2464
dfn-cert: DFN-CERT-2023-2463
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1753
dfn-cert: DFN-CERT-2023-1708
dfn-cert: DFN-CERT-2023-1707
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1634
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1528
dfn-cert: DFN-CERT-2023-1513
dfn-cert: DFN-CERT-2023-1499
dfn-cert: DFN-CERT-2023-1491
dfn-cert: DFN-CERT-2023-1490
dfn-cert: DFN-CERT-2023-1482
dfn-cert: DFN-CERT-2023-1473
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1319
dfn-cert: DFN-CERT-2023-1318
dfn-cert: DFN-CERT-2023-1315
dfn-cert: DFN-CERT-2023-1314
dfn-cert: DFN-CERT-2023-1313
dfn-cert: DFN-CERT-2023-1311
dfn-cert: DFN-CERT-2023-1307
dfn-cert: DFN-CERT-2023-1303
dfn-cert: DFN-CERT-2023-1286
dfn-cert: DFN-CERT-2023-1282
dfn-cert: DFN-CERT-2023-1281
dfn-cert: DFN-CERT-2023-1280
dfn-cert: DFN-CERT-2023-1262
dfn-cert: DFN-CERT-2023-1242
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-1128
dfn-cert: DFN-CERT-2023-1127
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1092
dfn-cert: DFN-CERT-2023-1091

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0996
dfn-cert: DFN-CERT-2023-0993
dfn-cert: DFN-CERT-2023-0919
dfn-cert: DFN-CERT-2023-0917
dfn-cert: DFN-CERT-2023-0906
dfn-cert: DFN-CERT-2023-0892
dfn-cert: DFN-CERT-2023-0891
dfn-cert: DFN-CERT-2023-0887
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0864
dfn-cert: DFN-CERT-2023-0863
dfn-cert: DFN-CERT-2023-0862
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0854
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0843
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0768
dfn-cert: DFN-CERT-2023-0759
dfn-cert: DFN-CERT-2023-0752
dfn-cert: DFN-CERT-2023-0751
dfn-cert: DFN-CERT-2023-0750
dfn-cert: DFN-CERT-2023-0749
dfn-cert: DFN-CERT-2023-0748
dfn-cert: DFN-CERT-2023-0739
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0692
dfn-cert: DFN-CERT-2023-0679
dfn-cert: DFN-CERT-2023-0678
dfn-cert: DFN-CERT-2023-0675
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0656
dfn-cert: DFN-CERT-2023-0632
dfn-cert: DFN-CERT-2023-0629
dfn-cert: DFN-CERT-2023-0612
dfn-cert: DFN-CERT-2023-0611
dfn-cert: DFN-CERT-2023-0603

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0600
dfn-cert: DFN-CERT-2023-0596
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-2023-0511
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2023-0500
dfn-cert: DFN-CERT-2023-0485
dfn-cert: DFN-CERT-2023-0483
dfn-cert: DFN-CERT-2023-0447
dfn-cert: DFN-CERT-2023-0423
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0378
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0355
dfn-cert: DFN-CERT-2023-0342
dfn-cert: DFN-CERT-2023-0341
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-2023-0269
dfn-cert: DFN-CERT-2023-0260
dfn-cert: DFN-CERT-2023-0255
dfn-cert: DFN-CERT-2023-0254
dfn-cert: DFN-CERT-2023-0194
dfn-cert: DFN-CERT-2023-0193
dfn-cert: DFN-CERT-2023-0192
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-2023-0086
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
dfn-cert: DFN-CERT-2022-2893

... continues on next page ...

... continued from previous page ...

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-2022-2447
dfn-cert: DFN-CERT-2022-2424
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2399
dfn-cert: DFN-CERT-2022-2370
dfn-cert: DFN-CERT-2022-2358
dfn-cert: DFN-CERT-2022-2357
dfn-cert: DFN-CERT-2022-2300
dfn-cert: DFN-CERT-2022-2291
dfn-cert: DFN-CERT-2022-2275
dfn-cert: DFN-CERT-2022-2274
dfn-cert: DFN-CERT-2022-2273
dfn-cert: DFN-CERT-2022-2265

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.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.12
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.12
```

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
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: `2024-02-02T04:09:01Z`

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
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-1175
cve: CVE-2023-1264
advisory_id: USN-5963-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0777
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-2023-2000
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1347
dfn-cert: DFN-CERT-2023-1019
dfn-cert: DFN-CERT-2023-0687
dfn-cert: DFN-CERT-2023-0686
dfn-cert: DFN-CERT-2023-0685
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-6027-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-6027-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.147.145

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the Traffic-Control Index (TCINDEX) implementation 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-2023-1281)
Jiasheng Jiang discovered that the HSA Linux kernel driver for AMD Radeon GPU devices did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2022-3108)
It was discovered that the infrared transceiver USB driver did not properly handle USB control messages. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (memory exhaustion). (CVE-2022-3903)
Haowei Yan discovered that a race condition existed in the Layer 2 Tunneling Protocol (L2TP) implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-4129)
It was discovered that the Human Interface Device (HID) support driver in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1073)
It was discovered that a memory leak existed in the SCTP protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2023-1074)
Lianhui Tang discovered that the MPLS implementation in the Linux kernel did not properly handle certain sysctl allocation failure conditions, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-26545)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6027-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6027.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6027-1`
`cve: CVE-2022-3108`
`cve: CVE-2022-3903`
`cve: CVE-2022-4129`
`cve: CVE-2023-1073`

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-1074
cve: CVE-2023-1281
cve: CVE-2023-26545
advisory_id: USN-6027-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-0787
cert-bund: WID-SEC-2023-0735
cert-bund: WID-SEC-2023-0684
cert-bund: WID-SEC-2023-0483
cert-bund: WID-SEC-2022-2322
cert-bund: WID-SEC-2022-2186
cert-bund: WID-SEC-2022-2038
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2024-0452
dfn-cert: DFN-CERT-2024-0332
dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2697
dfn-cert: DFN-CERT-2023-2690
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1829
dfn-cert: DFN-CERT-2023-1817
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1639
dfn-cert: DFN-CERT-2023-1635
dfn-cert: DFN-CERT-2023-1634
dfn-cert: DFN-CERT-2023-1597
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1406
dfn-cert: DFN-CERT-2023-1334
dfn-cert: DFN-CERT-2023-1313
dfn-cert: DFN-CERT-2023-1282
dfn-cert: DFN-CERT-2023-1281
dfn-cert: DFN-CERT-2023-1280

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1262
dfn-cert: DFN-CERT-2023-1181
dfn-cert: DFN-CERT-2023-1127
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1092
dfn-cert: DFN-CERT-2023-1091
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1002
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0996
dfn-cert: DFN-CERT-2023-0919
dfn-cert: DFN-CERT-2023-0918
dfn-cert: DFN-CERT-2023-0917
dfn-cert: DFN-CERT-2023-0916
dfn-cert: DFN-CERT-2023-0915
dfn-cert: DFN-CERT-2023-0906
dfn-cert: DFN-CERT-2023-0892
dfn-cert: DFN-CERT-2023-0891
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0873
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0759
dfn-cert: DFN-CERT-2023-0739
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0692
dfn-cert: DFN-CERT-2023-0676
dfn-cert: DFN-CERT-2023-0675
dfn-cert: DFN-CERT-2023-0674
dfn-cert: DFN-CERT-2023-0632
dfn-cert: DFN-CERT-2023-0612
dfn-cert: DFN-CERT-2023-0603
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0600
dfn-cert: DFN-CERT-2023-0596
dfn-cert: DFN-CERT-2023-0592
dfn-cert: DFN-CERT-2023-0586

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0582
dfn-cert: DFN-CERT-2023-0500
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2023-0355
dfn-cert: DFN-CERT-2023-0342
dfn-cert: DFN-CERT-2023-0194
dfn-cert: DFN-CERT-2023-0193
dfn-cert: DFN-CERT-2023-0192
dfn-cert: DFN-CERT-2023-0185
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2913
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2892
dfn-cert: DFN-CERT-2022-2891
dfn-cert: DFN-CERT-2022-2890
dfn-cert: DFN-CERT-2022-2879
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
dfn-cert: DFN-CERT-2022-2750

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6047-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-4.15, linux-azure-5.4, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-6047-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.148.146

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-4.15, linux-azure-5.4, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the Traffic-Control Index (TCINDEX) implementation in the Linux kernel did not properly perform filter deactivation in some situations. A local attacker could possibly use this to gain elevated privileges. Please note that with the fix for this CVE, kernel support for the TCINDEX classifier has been removed.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6047-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6047.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6047-1`
`cve: CVE-2023-1829`
`advisory_id: USN-6047-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-0953`
`dfn-cert: DFN-CERT-2024-1518`
`dfn-cert: DFN-CERT-2024-1508`
`dfn-cert: DFN-CERT-2024-1371`
`dfn-cert: DFN-CERT-2024-1369`
`dfn-cert: DFN-CERT-2024-1360`
`dfn-cert: DFN-CERT-2024-1359`
`dfn-cert: DFN-CERT-2024-1355`
`dfn-cert: DFN-CERT-2024-0983`
`dfn-cert: DFN-CERT-2024-0318`
`dfn-cert: DFN-CERT-2023-2927`
`dfn-cert: DFN-CERT-2023-2697`
`dfn-cert: DFN-CERT-2023-2690`
`dfn-cert: DFN-CERT-2023-2672`
`dfn-cert: DFN-CERT-2023-2668`
`dfn-cert: DFN-CERT-2023-2573`
`dfn-cert: DFN-CERT-2023-2339`
`dfn-cert: DFN-CERT-2023-2292`
`dfn-cert: DFN-CERT-2023-2279`
`dfn-cert: DFN-CERT-2023-2277`
`dfn-cert: DFN-CERT-2023-2264`
`dfn-cert: DFN-CERT-2023-2263`
`dfn-cert: DFN-CERT-2023-2237`
`dfn-cert: DFN-CERT-2023-2075`
`dfn-cert: DFN-CERT-2023-2033`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1829
dfn-cert: DFN-CERT-2023-1817
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1597
dfn-cert: DFN-CERT-2023-1563
dfn-cert: DFN-CERT-2023-1262
dfn-cert: DFN-CERT-2023-1181
dfn-cert: DFN-CERT-2023-1092
dfn-cert: DFN-CERT-2023-1091
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0980
dfn-cert: DFN-CERT-2023-0976
dfn-cert: DFN-CERT-2023-0975
dfn-cert: DFN-CERT-2023-0974
dfn-cert: DFN-CERT-2023-0920

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6094-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm' package(s) announced via the USN-6094-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.149.147

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm' package(s) on Ubuntu 18.04, Ubuntu 20.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-3707)

Jordy Zomer and Alexandra Sandulescu discovered that the Linux kernel did not properly implement speculative execution barriers in usercopy functions in certain situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2023-0459)

It was discovered that the TLS subsystem in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1075)

It was discovered that the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel contained a type confusion vulnerability in some situations. An attacker could use this to cause a denial of service (system crash). (CVE-2023-1078)

Xingyuan Mo discovered that the x86 KVM implementation in the Linux kernel did not properly initialize some data structures. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2023-1513)

It was discovered that a use-after-free vulnerability existed in the iSCSI TCP implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-2162)

It was discovered that the NET/ROM protocol implementation in the Linux kernel contained a race condition in some situations, 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-2023-32269)

Duoming Zhou discovered that a race condition existed in the infrared receiver/transceiver driver in the Linux kernel, leading to a use-after- free vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-1118)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6094-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6094.1

Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6094-1
cve: CVE-2022-3707
cve: CVE-2023-0459
cve: CVE-2023-1075
cve: CVE-2023-1078
cve: CVE-2023-1118
cve: CVE-2023-1513
cve: CVE-2023-2162
cve: CVE-2023-32269
advisory_id: USN-6094-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1305
cert-bund: WID-SEC-2023-1162
cert-bund: WID-SEC-2023-1003
cert-bund: WID-SEC-2023-0701
cert-bund: WID-SEC-2023-0684
cert-bund: WID-SEC-2023-0551
cert-bund: WID-SEC-2023-0543
cert-bund: WID-SEC-2022-1875
dfn-cert: DFN-CERT-2024-1537
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-0872
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0281
dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0247
dfn-cert: DFN-CERT-2024-0246
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2024-0097
dfn-cert: DFN-CERT-2024-0072
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2210
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1885
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1723
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1639
dfn-cert: DFN-CERT-2023-1597
dfn-cert: DFN-CERT-2023-1577
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1528
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1412
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1406
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1371
dfn-cert: DFN-CERT-2023-1370
dfn-cert: DFN-CERT-2023-1319
dfn-cert: DFN-CERT-2023-1318
dfn-cert: DFN-CERT-2023-1315
dfn-cert: DFN-CERT-2023-1314
dfn-cert: DFN-CERT-2023-1313
dfn-cert: DFN-CERT-2023-1303
dfn-cert: DFN-CERT-2023-1282
dfn-cert: DFN-CERT-2023-1281
dfn-cert: DFN-CERT-2023-1280
dfn-cert: DFN-CERT-2023-1263
dfn-cert: DFN-CERT-2023-1262
dfn-cert: DFN-CERT-2023-1182
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-1130
dfn-cert: DFN-CERT-2023-1128
dfn-cert: DFN-CERT-2023-1127
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1094
dfn-cert: DFN-CERT-2023-1085
dfn-cert: DFN-CERT-2023-1082
dfn-cert: DFN-CERT-2023-1081
dfn-cert: DFN-CERT-2023-1080
dfn-cert: DFN-CERT-2023-1079
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1002
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0952
dfn-cert: DFN-CERT-2023-0949
dfn-cert: DFN-CERT-2023-0948
dfn-cert: DFN-CERT-2023-0947
dfn-cert: DFN-CERT-2023-0944
dfn-cert: DFN-CERT-2023-0920
dfn-cert: DFN-CERT-2023-0919
dfn-cert: DFN-CERT-2023-0918

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0906
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0695
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0675
dfn-cert: DFN-CERT-2023-0674
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-2023-0592
dfn-cert: DFN-CERT-2023-0586
dfn-cert: DFN-CERT-2023-0582
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2914
dfn-cert: DFN-CERT-2022-2899
dfn-cert: DFN-CERT-2022-2878
dfn-cert: DFN-CERT-2022-2877
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6131-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-6131-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.150.148
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS

'linux, linux-aws, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, 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-2023-32233)

Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-31436)

Reima Ishii discovered that the nested KVM implementation for Intel x86 processors in the Linux kernel did not properly validate control registers in certain situations. An attacker in a guest VM could use this to cause a denial of service (guest crash). (CVE-2023-30456)

It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform data buffer size validation 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 expose sensitive information. (CVE-2023-1380)

Jean-Baptiste Cayrou discovered that the shiftfs file system in the Ubuntu Linux kernel contained a race condition when handling inode locking in some situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2023-2612)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6131-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6131.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-6131-1`
`cve: CVE-2023-1380`
`cve: CVE-2023-2612`
`cve: CVE-2023-30456`
`cve: CVE-2023-31436`
`cve: CVE-2023-32233`
`advisory_id: USN-6131-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1166`
`cert-bund: WID-SEC-2023-1095`
`cert-bund: WID-SEC-2023-0911`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-0637
dfn-cert: DFN-CERT-2024-0991
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0733
dfn-cert: DFN-CERT-2024-0728
dfn-cert: DFN-CERT-2024-0700
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0266
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0201
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2023-3003
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2682
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2478
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2198
dfn-cert: DFN-CERT-2023-2197
dfn-cert: DFN-CERT-2023-2173
dfn-cert: DFN-CERT-2023-2172
dfn-cert: DFN-CERT-2023-2145
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1953
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1848
dfn-cert: DFN-CERT-2023-1753
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1702
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1635
dfn-cert: DFN-CERT-2023-1634
dfn-cert: DFN-CERT-2023-1597
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1513
dfn-cert: DFN-CERT-2023-1501
dfn-cert: DFN-CERT-2023-1500
dfn-cert: DFN-CERT-2023-1499
dfn-cert: DFN-CERT-2023-1498
dfn-cert: DFN-CERT-2023-1492

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-1491
dfn-cert: DFN-CERT-2023-1490
dfn-cert: DFN-CERT-2023-1489
dfn-cert: DFN-CERT-2023-1482
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1473
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1447
dfn-cert: DFN-CERT-2023-1433
dfn-cert: DFN-CERT-2023-1432
dfn-cert: DFN-CERT-2023-1412
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1407
dfn-cert: DFN-CERT-2023-1405
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1371
dfn-cert: DFN-CERT-2023-1370
dfn-cert: DFN-CERT-2023-1353
dfn-cert: DFN-CERT-2023-1334
dfn-cert: DFN-CERT-2023-1307
dfn-cert: DFN-CERT-2023-1264
dfn-cert: DFN-CERT-2023-1263
dfn-cert: DFN-CERT-2023-1255
dfn-cert: DFN-CERT-2023-1242
dfn-cert: DFN-CERT-2023-1108
dfn-cert: DFN-CERT-2023-1064
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0920
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6172-1)

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-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gke-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-6172-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.152.149
```

... continues on next page ...

... continued from previous page ...

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-5.15, linux-gcp, linux-gcp-5.15, linux-gke, linux-gke-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 the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1076)
It was discovered that the Real-Time Scheduling Class implementation in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-1077)
It was discovered that the ASUS HID driver in the Linux kernel did not properly handle device removal, leading to a use-after-free vulnerability. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (system crash). (CVE-2023-1079)
It was discovered that the Xircom PCMCIA network device driver in the Linux kernel did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2023-1670)
It was discovered that a race condition existed in the Xen transport layer implementation for the 9P file system protocol in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (guest crash) or expose sensitive information (guest kernel memory). (CVE-2023-1859)
Jose Oliveira and Rodrigo Branco discovered that the Spectre Variant 2 mitigations with prctl syscall were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-1998)
It was discovered that the BigBen Interactive Kids' gamepad driver in the Linux kernel did not properly handle device removal, leading to a use- after-free vulnerability. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service (system crash). (CVE-2023-25012)
It was discovered that a use-after-free vulnerability existed in the HFS+ file system implementation in the Linux kernel. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-2985)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6172-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6172.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6172-1`
`cve: CVE-2023-1076`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2023-1077
cve: CVE-2023-1079
cve: CVE-2023-1670
cve: CVE-2023-1859
cve: CVE-2023-1998
cve: CVE-2023-25012
cve: CVE-2023-2985
advisory_id: USN-6172-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1981
cert-bund: WID-SEC-2023-1669
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1321
cert-bund: WID-SEC-2023-1063
cert-bund: WID-SEC-2023-0988
cert-bund: WID-SEC-2023-0805
cert-bund: WID-SEC-2023-0551
cert-bund: WID-SEC-2023-0260
dfn-cert: DFN-CERT-2024-1537
dfn-cert: DFN-CERT-2024-1060
dfn-cert: DFN-CERT-2024-1059
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0370
dfn-cert: DFN-CERT-2024-0304
dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0237
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2591
dfn-cert: DFN-CERT-2023-2543
dfn-cert: DFN-CERT-2023-2507
dfn-cert: DFN-CERT-2023-2506
dfn-cert: DFN-CERT-2023-2497
dfn-cert: DFN-CERT-2023-2496
dfn-cert: DFN-CERT-2023-2480
dfn-cert: DFN-CERT-2023-2465
dfn-cert: DFN-CERT-2023-2464
dfn-cert: DFN-CERT-2023-2463
dfn-cert: DFN-CERT-2023-2461
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2199
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2198
dfn-cert: DFN-CERT-2023-2197
dfn-cert: DFN-CERT-2023-2181
dfn-cert: DFN-CERT-2023-2174
dfn-cert: DFN-CERT-2023-2173
dfn-cert: DFN-CERT-2023-2172
dfn-cert: DFN-CERT-2023-2145
dfn-cert: DFN-CERT-2023-2106
dfn-cert: DFN-CERT-2023-2071
dfn-cert: DFN-CERT-2023-1993
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1797
dfn-cert: DFN-CERT-2023-1789
dfn-cert: DFN-CERT-2023-1770
dfn-cert: DFN-CERT-2023-1733
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1722
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1598
dfn-cert: DFN-CERT-2023-1597
dfn-cert: DFN-CERT-2023-1589
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1558
dfn-cert: DFN-CERT-2023-1542
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1407
dfn-cert: DFN-CERT-2023-1404
dfn-cert: DFN-CERT-2023-1403
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1370
dfn-cert: DFN-CERT-2023-1319
dfn-cert: DFN-CERT-2023-1242
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-1094

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1092
dfn-cert: DFN-CERT-2023-1091
dfn-cert: DFN-CERT-2023-1085
dfn-cert: DFN-CERT-2023-1082
dfn-cert: DFN-CERT-2023-1081
dfn-cert: DFN-CERT-2023-1080
dfn-cert: DFN-CERT-2023-1079
dfn-cert: DFN-CERT-2023-1076
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0976
dfn-cert: DFN-CERT-2023-0936
dfn-cert: DFN-CERT-2023-0920
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0586

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6193-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-aws-5.15, linux-azure, linux-azure-5.4, linux-azure-5.15, linux-azure-fde-5.15, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gcp-5.15, linux-gke, linux-gke-5.15, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.4, linux-hwe-5.15, linux-ibm, linux-ibm-5.4, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.4, linux-oracle-5.15, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-6193-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.153.150

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-aws-5.15, linux-azure, linux-azure-5.4, linux-azure-5.15, linux-azure-fde-5.15, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gcp-5.15, linux-gke, linux-gke-5.15, linux-gkeop, linux-gkeop-5.15, linux-hwe-5.4, linux-hwe-5.15, linux-ibm, linux-ibm-5.4, linux-kvm, linux-lowlatency, linux-lowlatency-hwe-5.15, linux-nvidia, linux-oracle, linux-oracle-5.4, linux-oracle-5.15, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight

Hangyu Hua discovered that the Flower classifier implementation in the Linux kernel contained an out-of-bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35788, LP: #2023577)
It was discovered that for some Intel processors the INVLPG instruction implementation did not properly flush global TLB entries when PCIDs are enabled. An attacker could use this to expose sensitive information (kernel memory) or possibly cause undesired behaviors. (LP: #2023220)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6193-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6193.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6193-1
url: https://launchpad.net/bugs/2023577
url: https://launchpad.net/bugs/2023220
cve: CVE-2023-35788
advisory_id: USN-6193-1
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-1504
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2480
dfn-cert: DFN-CERT-2023-2477
dfn-cert: DFN-CERT-2023-2217
dfn-cert: DFN-CERT-2023-2201
dfn-cert: DFN-CERT-2023-2078
dfn-cert: DFN-CERT-2023-2075
dfn-cert: DFN-CERT-2023-2033
dfn-cert: DFN-CERT-2023-2020
dfn-cert: DFN-CERT-2023-2019
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1776
dfn-cert: DFN-CERT-2023-1771
dfn-cert: DFN-CERT-2023-1770
dfn-cert: DFN-CERT-2023-1747
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1724
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1639
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1598
dfn-cert: DFN-CERT-2023-1589
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1552
dfn-cert: DFN-CERT-2023-1541
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1509
dfn-cert: DFN-CERT-2023-1504
dfn-cert: DFN-CERT-2023-1503

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6251-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6251-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.155.151

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3090)
Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges. (CVE-2023-32629)
It was discovered that the netfilter subsystem in the Linux kernel did not properly handle some error conditions, 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-2023-3390)
Tanguy Dubroca discovered that the netfilter subsystem in the Linux kernel did not properly handle certain pointer data type, leading to an out-of- bounds write vulnerability. A privileged attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-35001)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6251-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6251.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6251-1`
`cve: CVE-2023-3090`
`cve: CVE-2023-32629`
`cve: CVE-2023-3390`
`cve: CVE-2023-35001`
`advisory_id: USN-6251-1`
`cert-bund: WID-SEC-2023-2902`
`cert-bund: WID-SEC-2023-1903`
`cert-bund: WID-SEC-2023-1666`
`cert-bund: WID-SEC-2023-1595`
`dfn-cert: DFN-CERT-2024-0661`
`dfn-cert: DFN-CERT-2024-0657`
`dfn-cert: DFN-CERT-2024-0656`
`dfn-cert: DFN-CERT-2024-0094`
`dfn-cert: DFN-CERT-2023-3168`
`dfn-cert: DFN-CERT-2023-2792`
`dfn-cert: DFN-CERT-2023-2682`
`dfn-cert: DFN-CERT-2023-2669`
`dfn-cert: DFN-CERT-2023-2605`
`dfn-cert: DFN-CERT-2023-2582`
`dfn-cert: DFN-CERT-2023-2482`
`dfn-cert: DFN-CERT-2023-2480`
`dfn-cert: DFN-CERT-2023-2478`
`dfn-cert: DFN-CERT-2023-2477`
`dfn-cert: DFN-CERT-2023-2476`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2451
dfn-cert: DFN-CERT-2023-2380
dfn-cert: DFN-CERT-2023-2379
dfn-cert: DFN-CERT-2023-2340
dfn-cert: DFN-CERT-2023-2284
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-2217
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2207
dfn-cert: DFN-CERT-2023-2201
dfn-cert: DFN-CERT-2023-2199
dfn-cert: DFN-CERT-2023-2198
dfn-cert: DFN-CERT-2023-2197
dfn-cert: DFN-CERT-2023-2196
dfn-cert: DFN-CERT-2023-2182
dfn-cert: DFN-CERT-2023-2181
dfn-cert: DFN-CERT-2023-2174
dfn-cert: DFN-CERT-2023-2173
dfn-cert: DFN-CERT-2023-2172
dfn-cert: DFN-CERT-2023-2159
dfn-cert: DFN-CERT-2023-2145
dfn-cert: DFN-CERT-2023-2136
dfn-cert: DFN-CERT-2023-2106
dfn-cert: DFN-CERT-2023-2105
dfn-cert: DFN-CERT-2023-2078
dfn-cert: DFN-CERT-2023-2075
dfn-cert: DFN-CERT-2023-2033
dfn-cert: DFN-CERT-2023-2021
dfn-cert: DFN-CERT-2023-2019
dfn-cert: DFN-CERT-2023-2018
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-2016
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1872
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1797
dfn-cert: DFN-CERT-2023-1789
dfn-cert: DFN-CERT-2023-1781
dfn-cert: DFN-CERT-2023-1771
dfn-cert: DFN-CERT-2023-1770

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-1753
dfn-cert: DFN-CERT-2023-1739
dfn-cert: DFN-CERT-2023-1733
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1729
dfn-cert: DFN-CERT-2023-1723
dfn-cert: DFN-CERT-2023-1722
dfn-cert: DFN-CERT-2023-1721
dfn-cert: DFN-CERT-2023-1708
dfn-cert: DFN-CERT-2023-1707
dfn-cert: DFN-CERT-2023-1706
dfn-cert: DFN-CERT-2023-1703
dfn-cert: DFN-CERT-2023-1702
dfn-cert: DFN-CERT-2023-1672
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1622
dfn-cert: DFN-CERT-2023-1621
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1589
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1563
dfn-cert: DFN-CERT-2023-1558
dfn-cert: DFN-CERT-2023-1541
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6284-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-6284-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.156.152
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

It was discovered that the netlink implementation in the Linux kernel did not properly validate policies when parsing attributes in some situations. An attacker could use this to cause a denial of service (infinite recursion). (CVE-2020-36691)

Billy Jheng Bing Jhong discovered that the CIFS network file system implementation in the Linux kernel did not properly validate arguments to ioctl() in some situations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-0168)

It was discovered that the ext4 file system implementation in the Linux kernel contained a use-after-free vulnerability. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service (system crash). (CVE-2022-1184)

It was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using a return address from a sibling thread. A local attacker could possibly use this to expose sensitive information. (CVE-2022-27672)

William Zhao discovered that the Traffic Control (TC) subsystem in the Linux kernel did not properly handle network packet retransmission in certain situations. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2022-4269)

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)

It was discovered that a race condition existed in the btrfs file system 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 expose sensitive information. (CVE-2023-1611)

It was discovered that the APM X-Gene SoC hardware monitoring driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2023-1855)

It was discovered that the ST NCI NFC driver did not properly handle device removal events. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2023-1990)

It was discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation when mounting certain images. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service (system crash). (CVE-2023-2124)

It was discovered that the SLIMpro I2C device driver in the Linux kernel did not properly validate user-supplied data in some situations, leading to an out-of-bounds write vulnerability. A privileged attacker could use this to cause a denial of service ... [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-6284-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6284.1

Version used: `2024-02-02T04:09:01Z`

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-6284-1
cve: CVE-2020-36691
cve: CVE-2022-0168
cve: CVE-2022-1184
cve: CVE-2022-27672
cve: CVE-2022-4269
cve: CVE-2023-0590
cve: CVE-2023-1611
cve: CVE-2023-1855
cve: CVE-2023-1990
cve: CVE-2023-2124
cve: CVE-2023-2194
cve: CVE-2023-28466
cve: CVE-2023-30772
cve: CVE-2023-3111
cve: CVE-2023-3141
cve: CVE-2023-33203
advisory_id: USN-6284-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1410
cert-bund: WID-SEC-2023-1367
cert-bund: WID-SEC-2023-1250
cert-bund: WID-SEC-2023-1054
cert-bund: WID-SEC-2023-1002
cert-bund: WID-SEC-2023-0986
cert-bund: WID-SEC-2023-0962
cert-bund: WID-SEC-2023-0845
cert-bund: WID-SEC-2023-0752
cert-bund: WID-SEC-2023-0739
cert-bund: WID-SEC-2023-0669
cert-bund: WID-SEC-2023-0378
cert-bund: WID-SEC-2023-0322
cert-bund: WID-SEC-2022-2220
cert-bund: WID-SEC-2022-1215
cert-bund: WID-SEC-2022-1202
dfn-cert: DFN-CERT-2024-1037
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0516
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0370
dfn-cert: DFN-CERT-2024-0333

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0280
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2023-2916
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2744
dfn-cert: DFN-CERT-2023-2725
dfn-cert: DFN-CERT-2023-2721
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2482
dfn-cert: DFN-CERT-2023-2290
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2075
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-2037
dfn-cert: DFN-CERT-2023-2019
dfn-cert: DFN-CERT-2023-2018
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-2002
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1923
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1871
dfn-cert: DFN-CERT-2023-1870
dfn-cert: DFN-CERT-2023-1817
dfn-cert: DFN-CERT-2023-1753
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1729
dfn-cert: DFN-CERT-2023-1723
dfn-cert: DFN-CERT-2023-1722
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1639
dfn-cert: DFN-CERT-2023-1637
dfn-cert: DFN-CERT-2023-1622
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1599
dfn-cert: DFN-CERT-2023-1595
dfn-cert: DFN-CERT-2023-1589
dfn-cert: DFN-CERT-2023-1577

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1563
dfn-cert: DFN-CERT-2023-1558
dfn-cert: DFN-CERT-2023-1552
dfn-cert: DFN-CERT-2023-1541
dfn-cert: DFN-CERT-2023-1533
dfn-cert: DFN-CERT-2023-1513
dfn-cert: DFN-CERT-2023-1500
dfn-cert: DFN-CERT-2023-1499
dfn-cert: DFN-CERT-2023-1498
dfn-cert: DFN-CERT-2023-1492
dfn-cert: DFN-CERT-2023-1491
dfn-cert: DFN-CERT-2023-1490
dfn-cert: DFN-CERT-2023-1487
dfn-cert: DFN-CERT-2023-1476
dfn-cert: DFN-CERT-2023-1452
dfn-cert: DFN-CERT-2023-1447
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1412
dfn-cert: DFN-CERT-2023-1409
dfn-cert: DFN-CERT-2023-1407
dfn-cert: DFN-CERT-2023-1403
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1372
dfn-cert: DFN-CERT-2023-1371
dfn-cert: DFN-CERT-2023-1370
dfn-cert: DFN-CERT-2023-1262
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-1128
dfn-cert: DFN-CERT-2023-1127
dfn-cert: DFN-CERT-2023-1100
dfn-cert: DFN-CERT-2023-1094
dfn-cert: DFN-CERT-2023-1085
dfn-cert: DFN-CERT-2023-1082
dfn-cert: DFN-CERT-2023-1081
dfn-cert: DFN-CERT-2023-1080
dfn-cert: DFN-CERT-2023-1079
dfn-cert: DFN-CERT-2023-1076
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-1006
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0952
dfn-cert: DFN-CERT-2023-0948
dfn-cert: DFN-CERT-2023-0944
dfn-cert: DFN-CERT-2023-0920
dfn-cert: DFN-CERT-2023-0906

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0878
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
dfn-cert: DFN-CERT-2023-0873
dfn-cert: DFN-CERT-2023-0848
dfn-cert: DFN-CERT-2023-0795
dfn-cert: DFN-CERT-2023-0794
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0752
dfn-cert: DFN-CERT-2023-0739
dfn-cert: DFN-CERT-2023-0729
dfn-cert: DFN-CERT-2023-0726
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0678
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0632
dfn-cert: DFN-CERT-2023-0606
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-2023-0573
dfn-cert: DFN-CERT-2023-0572
dfn-cert: DFN-CERT-2023-0534
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2023-0500
dfn-cert: DFN-CERT-2023-0447
dfn-cert: DFN-CERT-2023-0393
dfn-cert: DFN-CERT-2023-0339
dfn-cert: DFN-CERT-2023-0127
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2834
dfn-cert: DFN-CERT-2022-2710
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2449
dfn-cert: DFN-CERT-2022-2326
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2022-2062
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1424

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1278
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6317-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-hwe-5.4, linux-kvm, linux-oracle, linux-xilinx-zynqmp' package(s) announced via the USN-6317-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.159.154
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-gcp, linux-hwe-5.4, linux-kvm, linux-oracle, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Daniel Moghimi discovered that some Intel(R) Processors did not properly clear microarchitectural state after speculative execution of various instructions. A local unprivileged user could use this to obtain to sensitive information. (CVE-2022-40982)
Tavis Ormandy discovered that some AMD processors did not properly handle speculative execution of certain vector register instructions. A local attacker could use this to expose sensitive information. (CVE-2023-20593)
It was discovered that the universal 32bit network packet classifier implementation in the Linux kernel did not properly perform reference counting in some situations, 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-2023-3609)

... continues on next page ...

... continued from previous page ...

It was discovered that the Quick Fair Queueing network scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-3611)
It was discovered that the network packet classifier with netfilter/firewall marks implementation in the Linux kernel did not properly handle reference counting, 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-2023-3776)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6317-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6317.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6317-1`
`cve: CVE-2022-40982`
`cve: CVE-2023-20593`
`cve: CVE-2023-3609`
`cve: CVE-2023-3611`
`cve: CVE-2023-3776`
`advisory_id: USN-6317-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2902`
`cert-bund: WID-SEC-2023-2679`
`cert-bund: WID-SEC-2023-2007`
`cert-bund: WID-SEC-2023-1873`
`cert-bund: WID-SEC-2023-1862`
`dfn-cert: DFN-CERT-2024-1399`
`dfn-cert: DFN-CERT-2024-1011`
`dfn-cert: DFN-CERT-2024-0991`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0733`
`dfn-cert: DFN-CERT-2024-0661`
`dfn-cert: DFN-CERT-2024-0657`
`dfn-cert: DFN-CERT-2024-0656`
`dfn-cert: DFN-CERT-2024-0527`
`dfn-cert: DFN-CERT-2024-0281`
`dfn-cert: DFN-CERT-2024-0280`
`dfn-cert: DFN-CERT-2024-0266`
`dfn-cert: DFN-CERT-2024-0249`
`dfn-cert: DFN-CERT-2024-0246`
`dfn-cert: DFN-CERT-2024-0201`
`dfn-cert: DFN-CERT-2024-0139`
`dfn-cert: DFN-CERT-2024-0105`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2023-3168
dfn-cert: DFN-CERT-2023-3045
dfn-cert: DFN-CERT-2023-3003
dfn-cert: DFN-CERT-2023-2990
dfn-cert: DFN-CERT-2023-2986
dfn-cert: DFN-CERT-2023-2984
dfn-cert: DFN-CERT-2023-2972
dfn-cert: DFN-CERT-2023-2927
dfn-cert: DFN-CERT-2023-2925
dfn-cert: DFN-CERT-2023-2924
dfn-cert: DFN-CERT-2023-2923
dfn-cert: DFN-CERT-2023-2919
dfn-cert: DFN-CERT-2023-2916
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2866
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2548
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2483
dfn-cert: DFN-CERT-2023-2478
dfn-cert: DFN-CERT-2023-2451
dfn-cert: DFN-CERT-2023-2379
dfn-cert: DFN-CERT-2023-2353
dfn-cert: DFN-CERT-2023-2342
dfn-cert: DFN-CERT-2023-2340
dfn-cert: DFN-CERT-2023-2292
dfn-cert: DFN-CERT-2023-2290
dfn-cert: DFN-CERT-2023-2279
dfn-cert: DFN-CERT-2023-2278
dfn-cert: DFN-CERT-2023-2277
dfn-cert: DFN-CERT-2023-2274
dfn-cert: DFN-CERT-2023-2264
dfn-cert: DFN-CERT-2023-2217
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2210
dfn-cert: DFN-CERT-2023-2201
dfn-cert: DFN-CERT-2023-2136
dfn-cert: DFN-CERT-2023-2123
dfn-cert: DFN-CERT-2023-2112
dfn-cert: DFN-CERT-2023-2103
dfn-cert: DFN-CERT-2023-2071
dfn-cert: DFN-CERT-2023-2070
dfn-cert: DFN-CERT-2023-2038

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2037
dfn-cert: DFN-CERT-2023-2020
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-2016
dfn-cert: DFN-CERT-2023-2009
dfn-cert: DFN-CERT-2023-2008
dfn-cert: DFN-CERT-2023-2007
dfn-cert: DFN-CERT-2023-2006
dfn-cert: DFN-CERT-2023-1993
dfn-cert: DFN-CERT-2023-1968
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1953
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1898
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1885
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1872
dfn-cert: DFN-CERT-2023-1866
dfn-cert: DFN-CERT-2023-1864
dfn-cert: DFN-CERT-2023-1862
dfn-cert: DFN-CERT-2023-1859
dfn-cert: DFN-CERT-2023-1857
dfn-cert: DFN-CERT-2023-1849
dfn-cert: DFN-CERT-2023-1847
dfn-cert: DFN-CERT-2023-1841
dfn-cert: DFN-CERT-2023-1797
dfn-cert: DFN-CERT-2023-1789
dfn-cert: DFN-CERT-2023-1781
dfn-cert: DFN-CERT-2023-1767
dfn-cert: DFN-CERT-2023-1739
dfn-cert: DFN-CERT-2023-1733
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1682

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5995-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5995-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   vim
Installed version:    vim-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-2:8.1.2269-1ubuntu5.13
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:8.1.2269-1ubuntu5
Fixed version:      >=vim-tiny-2:8.1.2269-1ubuntu5.13
```

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

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

Vulnerability Insight
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possible execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-0413, CVE-2022-1629, CVE-2022-1674, CVE-2022-1733, CVE-2022-1735, CVE-2022-1785, CVE-2022-1796, CVE-2022-1851, CVE-2022-1898, CVE-2022-1942, CVE-2022-1968, CVE-2022-2124, CVE-2022-2125, CVE-2022-2126, CVE-2022-2129, CVE-2022-2175, CVE-2022-2183, CVE-2022-2206, CVE-2022-2304, CVE-2022-2345, CVE-2022-2581)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possible execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-1720, CVE-2022-2571, CVE-2022-2845, CVE-2022-2849, CVE-2022-2923)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possible execute arbitrary code. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-1927, CVE-2022-2344)
It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possible execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-2946)

... continues on next page ...

... continued from previous page ...

It was discovered that Vim incorrectly handled memory when opening certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash, or possible execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-2980)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5995-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.5995.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5995-1`
`cve: CVE-2022-0413`
`cve: CVE-2022-1629`
`cve: CVE-2022-1674`
`cve: CVE-2022-1720`
`cve: CVE-2022-1733`
`cve: CVE-2022-1735`
`cve: CVE-2022-1785`
`cve: CVE-2022-1796`
`cve: CVE-2022-1851`
`cve: CVE-2022-1898`
`cve: CVE-2022-1927`
`cve: CVE-2022-1942`
`cve: CVE-2022-1968`
`cve: CVE-2022-2124`
`cve: CVE-2022-2125`
`cve: CVE-2022-2126`
`cve: CVE-2022-2129`
`cve: CVE-2022-2175`
`cve: CVE-2022-2183`
`cve: CVE-2022-2206`
`cve: CVE-2022-2304`
`cve: CVE-2022-2344`
`cve: CVE-2022-2345`
`cve: CVE-2022-2571`
`cve: CVE-2022-2581`
`cve: CVE-2022-2845`
`cve: CVE-2022-2849`
`cve: CVE-2022-2923`
`cve: CVE-2022-2946`
`cve: CVE-2022-2980`
`advisory_id: USN-5995-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0561`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1846
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1195
cert-bund: WID-SEC-2022-1157
cert-bund: WID-SEC-2022-1148
cert-bund: WID-SEC-2022-1076
cert-bund: WID-SEC-2022-1073
cert-bund: WID-SEC-2022-0926
cert-bund: WID-SEC-2022-0880
cert-bund: WID-SEC-2022-0776
cert-bund: WID-SEC-2022-0630
cert-bund: WID-SEC-2022-0583
cert-bund: WID-SEC-2022-0509
cert-bund: WID-SEC-2022-0473
cert-bund: WID-SEC-2022-0459
cert-bund: WID-SEC-2022-0440
cert-bund: WID-SEC-2022-0415
cert-bund: WID-SEC-2022-0397
cert-bund: WID-SEC-2022-0364
cert-bund: WID-SEC-2022-0363
cert-bund: WID-SEC-2022-0362
cert-bund: WID-SEC-2022-0271
cert-bund: WID-SEC-2022-0132
cert-bund: WID-SEC-2022-0131
cert-bund: WID-SEC-2022-0130
cert-bund: WID-SEC-2022-0126
cert-bund: WID-SEC-2022-0057
cert-bund: CB-K22/0622
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0853
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2022-2819
dfn-cert: DFN-CERT-2022-2716
dfn-cert: DFN-CERT-2022-2675
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2565
dfn-cert: DFN-CERT-2022-2517
dfn-cert: DFN-CERT-2022-2364
dfn-cert: DFN-CERT-2022-1995
dfn-cert: DFN-CERT-2022-1887
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1718
dfn-cert: DFN-CERT-2022-1657
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1544
dfn-cert: DFN-CERT-2022-1526

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1474
dfn-cert: DFN-CERT-2022-1466
dfn-cert: DFN-CERT-2022-1461
dfn-cert: DFN-CERT-2022-1443
dfn-cert: DFN-CERT-2022-1381
dfn-cert: DFN-CERT-2022-1367
dfn-cert: DFN-CERT-2022-1257
dfn-cert: DFN-CERT-2022-1237
dfn-cert: DFN-CERT-2022-1150
dfn-cert: DFN-CERT-2022-1128
dfn-cert: DFN-CERT-2022-1118
dfn-cert: DFN-CERT-2022-1031
dfn-cert: DFN-CERT-2022-0598
dfn-cert: DFN-CERT-2022-0503
dfn-cert: DFN-CERT-2022-0291

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6387-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6387-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.163.160

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Jana Hofmann, Emanuele Vannacci, Cedric Fournet, Boris Kopf, and Oleksii Oleksenko discovered that some AMD processors could leak stale data from division operations in certain situations. A local attacker could possibly use this to expose sensitive information. (CVE-2023-20588)
It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle L2CAP socket release, 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-2023-40283)
It was discovered that some network classifier implementations in the Linux kernel contained use-after-free vulnerabilities. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4128)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6387-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6387.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6387-1`
`cve: CVE-2023-20588`
`cve: CVE-2023-40283`
`cve: CVE-2023-4128`
`advisory_id: USN-6387-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2023-3137`
`cert-bund: WID-SEC-2023-2054`
`cert-bund: WID-SEC-2023-2042`
`cert-bund: WID-SEC-2023-2001`
`dfn-cert: DFN-CERT-2024-1183`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0745`
`dfn-cert: DFN-CERT-2024-0661`
`dfn-cert: DFN-CERT-2024-0656`
`dfn-cert: DFN-CERT-2024-0481`
`dfn-cert: DFN-CERT-2024-0452`
`dfn-cert: DFN-CERT-2024-0333`
`dfn-cert: DFN-CERT-2024-0260`
`dfn-cert: DFN-CERT-2024-0250`
`dfn-cert: DFN-CERT-2024-0248`
`dfn-cert: DFN-CERT-2024-0237`
`dfn-cert: DFN-CERT-2024-0235`
`dfn-cert: DFN-CERT-2024-0139`
`dfn-cert: DFN-CERT-2024-0105`
`dfn-cert: DFN-CERT-2024-0094`
`dfn-cert: DFN-CERT-2024-0082`
`dfn-cert: DFN-CERT-2023-3100`
`dfn-cert: DFN-CERT-2023-3003`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2990
dfn-cert: DFN-CERT-2023-2986
dfn-cert: DFN-CERT-2023-2925
dfn-cert: DFN-CERT-2023-2924
dfn-cert: DFN-CERT-2023-2923
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2883
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2717
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2621
dfn-cert: DFN-CERT-2023-2591
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2548
dfn-cert: DFN-CERT-2023-2543
dfn-cert: DFN-CERT-2023-2508
dfn-cert: DFN-CERT-2023-2497
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2483
dfn-cert: DFN-CERT-2023-2482
dfn-cert: DFN-CERT-2023-2480
dfn-cert: DFN-CERT-2023-2479
dfn-cert: DFN-CERT-2023-2477
dfn-cert: DFN-CERT-2023-2476
dfn-cert: DFN-CERT-2023-2463
dfn-cert: DFN-CERT-2023-2461
dfn-cert: DFN-CERT-2023-2451
dfn-cert: DFN-CERT-2023-2442
dfn-cert: DFN-CERT-2023-2438
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2342
dfn-cert: DFN-CERT-2023-2321
dfn-cert: DFN-CERT-2023-2290
dfn-cert: DFN-CERT-2023-2288
dfn-cert: DFN-CERT-2023-2266
dfn-cert: DFN-CERT-2023-2219
dfn-cert: DFN-CERT-2023-2218
dfn-cert: DFN-CERT-2023-2214
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2212
dfn-cert: DFN-CERT-2023-2211
dfn-cert: DFN-CERT-2023-2210
dfn-cert: DFN-CERT-2023-2209
dfn-cert: DFN-CERT-2023-2208
dfn-cert: DFN-CERT-2023-2163

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2162
dfn-cert: DFN-CERT-2023-2161
dfn-cert: DFN-CERT-2023-2103
dfn-cert: DFN-CERT-2023-2080
dfn-cert: DFN-CERT-2023-2016
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1873
dfn-cert: DFN-CERT-2023-1839

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6441-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6441-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.165.162

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Ross Lagerwall discovered that the Xen netback backend driver in the Linux kernel did not properly handle certain unusual packets from a paravirtualized network frontend, leading to a buffer overflow. An attacker in a guest VM could use this to cause a denial of service (host system crash) or possibly execute arbitrary code. (CVE-2023-34319)
Kyle Zeng discovered that the networking stack implementation in the Linux kernel did not properly validate skb object size in certain conditions. An attacker could use this cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42752)
Kyle Zeng discovered that the netfiler subsystem in the Linux kernel did not properly calculate array offsets, leading to a out-of-bounds write vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-42753)

... continues on next page ...

... continued from previous page ...

Kyle Zeng discovered that the IPv4 Resource Reservation Protocol (RSVP) classifier implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service (system crash). Please note that kernel packet classifier support for RSVP has been removed to resolve this vulnerability. (CVE-2023-42755)
Kyle Zeng discovered that the netfilter subsystem in the Linux kernel contained a race condition in IP set operations in certain situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-42756)
Bing-Jhong Billy Jheng discovered that the Unix domain socket implementation in the Linux kernel contained a race condition in certain situations, 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-2023-4622)
Budimir Markovic discovered that the qdisc implementation in the Linux kernel did not properly validate inner classes, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4623)
Alex Birnberg discovered that the netfilter subsystem in the Linux kernel did not properly validate register length, leading to an out-of- bounds write vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-4881)
It was discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel did not properly handle network packets in certain conditions, 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-2023-4921)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6441-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6441.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6441-1`
`cve: CVE-2023-34319`
`cve: CVE-2023-42752`
`cve: CVE-2023-42753`
`cve: CVE-2023-42755`
`cve: CVE-2023-42756`
`cve: CVE-2023-4622`
`cve: CVE-2023-4623`
`cve: CVE-2023-4881`
`cve: CVE-2023-4921`
`advisory_id: USN-6441-1`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-1046`
`cert-bund: WID-SEC-2023-2503`
`cert-bund: WID-SEC-2023-2441`
`cert-bund: WID-SEC-2023-2434`
`cert-bund: WID-SEC-2023-2386`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2316
cert-bund: WID-SEC-2023-2307
cert-bund: WID-SEC-2023-2284
cert-bund: WID-SEC-2023-2018
dfn-cert: DFN-CERT-2024-1518
dfn-cert: DFN-CERT-2024-1508
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1218
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1087
dfn-cert: DFN-CERT-2024-1075
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-0991
dfn-cert: DFN-CERT-2024-0973
dfn-cert: DFN-CERT-2024-0951
dfn-cert: DFN-CERT-2024-0941
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0728
dfn-cert: DFN-CERT-2024-0700
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0657
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0655
dfn-cert: DFN-CERT-2024-0555
dfn-cert: DFN-CERT-2024-0527
dfn-cert: DFN-CERT-2024-0510
dfn-cert: DFN-CERT-2024-0505
dfn-cert: DFN-CERT-2024-0504
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0452
dfn-cert: DFN-CERT-2024-0448
dfn-cert: DFN-CERT-2024-0432
dfn-cert: DFN-CERT-2024-0431
dfn-cert: DFN-CERT-2024-0428
dfn-cert: DFN-CERT-2024-0413
dfn-cert: DFN-CERT-2024-0410
dfn-cert: DFN-CERT-2024-0358
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0304
dfn-cert: DFN-CERT-2024-0281
dfn-cert: DFN-CERT-2024-0280

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0266
dfn-cert: DFN-CERT-2024-0260
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2024-0248
dfn-cert: DFN-CERT-2024-0247
dfn-cert: DFN-CERT-2024-0246
dfn-cert: DFN-CERT-2024-0213
dfn-cert: DFN-CERT-2024-0201
dfn-cert: DFN-CERT-2024-0200
dfn-cert: DFN-CERT-2024-0198
dfn-cert: DFN-CERT-2024-0097
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0072
dfn-cert: DFN-CERT-2024-0064
dfn-cert: DFN-CERT-2023-3155
dfn-cert: DFN-CERT-2023-3147
dfn-cert: DFN-CERT-2023-3138
dfn-cert: DFN-CERT-2023-3137
dfn-cert: DFN-CERT-2023-3136
dfn-cert: DFN-CERT-2023-3135
dfn-cert: DFN-CERT-2023-3131
dfn-cert: DFN-CERT-2023-3003
dfn-cert: DFN-CERT-2023-2990
dfn-cert: DFN-CERT-2023-2986
dfn-cert: DFN-CERT-2023-2923
dfn-cert: DFN-CERT-2023-2919
dfn-cert: DFN-CERT-2023-2916
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2690
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2683
dfn-cert: DFN-CERT-2023-2682
dfn-cert: DFN-CERT-2023-2672
dfn-cert: DFN-CERT-2023-2671
dfn-cert: DFN-CERT-2023-2669
dfn-cert: DFN-CERT-2023-2668
dfn-cert: DFN-CERT-2023-2642
dfn-cert: DFN-CERT-2023-2621
dfn-cert: DFN-CERT-2023-2620
dfn-cert: DFN-CERT-2023-2607
dfn-cert: DFN-CERT-2023-2606
dfn-cert: DFN-CERT-2023-2605
dfn-cert: DFN-CERT-2023-2591
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2580

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2579
dfn-cert: DFN-CERT-2023-2578
dfn-cert: DFN-CERT-2023-2577
dfn-cert: DFN-CERT-2023-2576
dfn-cert: DFN-CERT-2023-2575
dfn-cert: DFN-CERT-2023-2574
dfn-cert: DFN-CERT-2023-2543
dfn-cert: DFN-CERT-2023-2510
dfn-cert: DFN-CERT-2023-2508
dfn-cert: DFN-CERT-2023-2507
dfn-cert: DFN-CERT-2023-2506
dfn-cert: DFN-CERT-2023-2497
dfn-cert: DFN-CERT-2023-2496
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2466
dfn-cert: DFN-CERT-2023-2465
dfn-cert: DFN-CERT-2023-2464
dfn-cert: DFN-CERT-2023-2463
dfn-cert: DFN-CERT-2023-2461
dfn-cert: DFN-CERT-2023-2438
dfn-cert: DFN-CERT-2023-2426
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2389
dfn-cert: DFN-CERT-2023-2282
dfn-cert: DFN-CERT-2023-2257
dfn-cert: DFN-CERT-2023-2218
dfn-cert: DFN-CERT-2023-2163
dfn-cert: DFN-CERT-2023-2162
dfn-cert: DFN-CERT-2023-2161
dfn-cert: DFN-CERT-2023-2103
dfn-cert: DFN-CERT-2023-2080
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1841
dfn-cert: DFN-CERT-2023-1823

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5689-1)

Summary
The remote host is missing an update for the 'perl' package(s) announced via the USN-5689-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: perl
Installed version: perl-5.30.0-9ubuntu0.2
Fixed version: >=perl-5.30.0-9ubuntu0.3

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

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

Vulnerability Insight
It was discovered that Perl incorrectly handled certain signature verification. An remote attacker could possibly use this issue to bypass signature verification.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5689-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5689.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5689-1
cve: CVE-2020-16156
advisory_id: USN-5689-1
cert-bund: WID-SEC-2023-0138
dfn-cert: DFN-CERT-2022-0007

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6655-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-6655-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: binutils
Installed version: binutils-2.34-6ubuntu1.1
Fixed version: >=binutils-2.34-6ubuntu1.9

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
It was discovered that GNU binutils was not properly handling the logic behind certain memory management related operations, which could lead to an invalid memory access. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-47695)
It was discovered that GNU binutils was not properly performing bounds checks when dealing with memory allocation operations, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-48063)
It was discovered that GNU binutils incorrectly handled memory management operations in several of its functions, which could lead to excessive memory consumption due to memory leaks. An attacker could possibly use these issues to cause a denial of service. (CVE-2022-48065)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6655-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6655.1
Version used: `2024-02-27T04:09:22Z`

References
`url: https://ubuntu.com/security/notices/USN-6655-1`
`cve: CVE-2022-47695`
`cve: CVE-2022-48063`
`cve: CVE-2022-48065`
`advisory_id: USN-6655-1`
`cert-bund: WID-SEC-2023-2165`
`cert-bund: WID-SEC-2023-2114`
`dfn-cert: DFN-CERT-2024-0497`
`dfn-cert: DFN-CERT-2023-2526`
`dfn-cert: DFN-CERT-2023-2386`
`dfn-cert: DFN-CERT-2023-2222`
`dfn-cert: DFN-CERT-2023-2183`

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6605-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6605-1 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-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.170.168
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Lin Ma discovered that the netfilter subsystem in the Linux kernel did not properly validate network family support while creating a new netfilter table. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6040)
It was discovered that the CIFS network file system implementation in the Linux kernel did not properly validate the server frame size in certain situation, leading to an out-of-bounds read vulnerability. An attacker could use this to construct a malicious CIFS image that, when operated on, could cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-6606)
Budimir Markovic, Lucas De Marchi, and Pengfei Xu discovered that the perf subsystem in the Linux kernel did not properly validate all event sizes when attaching new events, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-6931)
It was discovered that the IGMP protocol implementation in the Linux kernel contained a race condition, 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-2023-6932)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6605-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6605.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6605-1
cve: CVE-2023-6040
cve: CVE-2023-6606
cve: CVE-2023-6931
cve: CVE-2023-6932
advisory_id: USN-6605-1
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0072
cert-bund: WID-SEC-2023-3181
cert-bund: WID-SEC-2023-3087
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1357
dfn-cert: DFN-CERT-2024-1353
dfn-cert: DFN-CERT-2024-1346
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1019
dfn-cert: DFN-CERT-2024-0945
dfn-cert: DFN-CERT-2024-0870
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0679
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0654
dfn-cert: DFN-CERT-2024-0603
dfn-cert: DFN-CERT-2024-0540
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0463
dfn-cert: DFN-CERT-2024-0461
dfn-cert: DFN-CERT-2024-0452
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-2024-0396
dfn-cert: DFN-CERT-2024-0351
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0332
dfn-cert: DFN-CERT-2024-0324
dfn-cert: DFN-CERT-2024-0321
dfn-cert: DFN-CERT-2024-0318
dfn-cert: DFN-CERT-2024-0308
dfn-cert: DFN-CERT-2024-0307
dfn-cert: DFN-CERT-2024-0243
dfn-cert: DFN-CERT-2024-0241
dfn-cert: DFN-CERT-2024-0240

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0239
dfn-cert: DFN-CERT-2024-0238
dfn-cert: DFN-CERT-2024-0237
dfn-cert: DFN-CERT-2024-0236
dfn-cert: DFN-CERT-2024-0235
dfn-cert: DFN-CERT-2024-0223
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0142
dfn-cert: DFN-CERT-2024-0123
dfn-cert: DFN-CERT-2024-0121
dfn-cert: DFN-CERT-2024-0095
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0015
dfn-cert: DFN-CERT-2024-0009

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6648-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6648-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.172.170

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that a race condition existed in the AppleTalk networking subsystem of 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-2023-51781)

... continues on next page ...

... continued from previous page ...

Zhenghan Wang discovered that the generic ID allocator implementation in the Linux kernel did not properly check for null bitmap when releasing IDs. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-6915)
Robert Morris discovered that the CIFS network file system implementation in the Linux kernel did not properly validate certain server commands fields, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2024-0565)
Jann Horn discovered that the TLS subsystem in the Linux kernel did not properly handle spliced messages, leading to an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2024-0646)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6648-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6648.1
Version used: `2024-02-23T04:08:56Z`

References
`url: https://ubuntu.com/security/notices/USN-6648-1`
`cve: CVE-2023-51781`
`cve: CVE-2023-6915`
`cve: CVE-2024-0565`
`cve: CVE-2024-0646`
`advisory_id: USN-6648-1`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0136`
`cert-bund: WID-SEC-2024-0097`
`cert-bund: WID-SEC-2024-0086`
`cert-bund: WID-SEC-2024-0017`
`dfn-cert: DFN-CERT-2024-1512`
`dfn-cert: DFN-CERT-2024-1398`
`dfn-cert: DFN-CERT-2024-1381`
`dfn-cert: DFN-CERT-2024-1176`
`dfn-cert: DFN-CERT-2024-1165`
`dfn-cert: DFN-CERT-2024-1060`
`dfn-cert: DFN-CERT-2024-0973`
`dfn-cert: DFN-CERT-2024-0972`
`dfn-cert: DFN-CERT-2024-0949`
`dfn-cert: DFN-CERT-2024-0941`
`dfn-cert: DFN-CERT-2024-0925`
`dfn-cert: DFN-CERT-2024-0870`
`dfn-cert: DFN-CERT-2024-0809`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0745`
`dfn-cert: DFN-CERT-2024-0733`
`dfn-cert: DFN-CERT-2024-0730`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2024-0729
dfn-cert: DFN-CERT-2024-0679
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0657
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0654
dfn-cert: DFN-CERT-2024-0603
dfn-cert: DFN-CERT-2024-0488
dfn-cert: DFN-CERT-2024-0487
dfn-cert: DFN-CERT-2024-0486
dfn-cert: DFN-CERT-2024-0485
dfn-cert: DFN-CERT-2024-0481
dfn-cert: DFN-CERT-2024-0468
dfn-cert: DFN-CERT-2024-0452
dfn-cert: DFN-CERT-2024-0448
dfn-cert: DFN-CERT-2024-0432
dfn-cert: DFN-CERT-2024-0431
dfn-cert: DFN-CERT-2024-0428
dfn-cert: DFN-CERT-2024-0427
dfn-cert: DFN-CERT-2024-0414
dfn-cert: DFN-CERT-2024-0413
dfn-cert: DFN-CERT-2024-0410
dfn-cert: DFN-CERT-2024-0407
dfn-cert: DFN-CERT-2024-0403
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0332
dfn-cert: DFN-CERT-2024-0138
dfn-cert: DFN-CERT-2024-0095
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0015
dfn-cert: DFN-CERT-2024-0009
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6681-1)

Summary
The remote host is missing an update for the 'linux, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-iot, linux-kvm, linux-raspi' package(s) announced via the USN-6681-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.173.171
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'linux, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-iot, linux-kvm, linux-raspi' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Wenqing Liu discovered that the f2fs file system implementation in the Linux kernel did not properly validate inode types while performing garbage collection. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2021-44879)
It was discovered that the DesignWare USB3 for Qualcomm SoCs driver in the Linux kernel did not properly handle certain error conditions during device registration. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-22995)
Bien Pham discovered that the netfiler subsystem in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local user could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-4244)
It was discovered that a race condition existed in the Bluetooth subsystem of 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-2023-51779)
It was discovered that a race condition existed in the ATM (Asynchronous Transfer Mode) subsystem of 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-2023-51780)
It was discovered that a race condition existed in the Rose X.25 protocol 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-2023-51782)
Alon Zahavi discovered that the NVMe-oF/TCP subsystem of the Linux kernel did not properly handle connect command payloads in certain situations, leading to an out-of-bounds read vulnerability. A remote attacker could use this to expose sensitive information (kernel memory). (CVE-2023-6121)
It was discovered that the VirtIO subsystem in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to possibly expose sensitive information (kernel memory). (CVE-2024-0340)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6681-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6681.1
Version used: `2024-03-07T04:08:56Z`

References
`url: https://ubuntu.com/security/notices/USN-6681-1`
`cve: CVE-2021-44879`

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-22995
cve: CVE-2023-4244
cve: CVE-2023-51779
cve: CVE-2023-51780
cve: CVE-2023-51782
cve: CVE-2023-6121
cve: CVE-2024-0340
advisory_id: USN-6681-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0073
cert-bund: WID-SEC-2024-0032
cert-bund: WID-SEC-2024-0017
cert-bund: WID-SEC-2024-0015
cert-bund: WID-SEC-2023-2953
cert-bund: WID-SEC-2023-2284
cert-bund: WID-SEC-2023-0494
cert-bund: WID-SEC-2022-0061
cert-bund: CB-K22/0181
dfn-cert: DFN-CERT-2024-1542
dfn-cert: DFN-CERT-2024-1541
dfn-cert: DFN-CERT-2024-1478
dfn-cert: DFN-CERT-2024-1427
dfn-cert: DFN-CERT-2024-1426
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1060
dfn-cert: DFN-CERT-2024-1059
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0946
dfn-cert: DFN-CERT-2024-0848
dfn-cert: DFN-CERT-2024-0841
dfn-cert: DFN-CERT-2024-0837
dfn-cert: DFN-CERT-2024-0814
dfn-cert: DFN-CERT-2024-0802
dfn-cert: DFN-CERT-2024-0801
dfn-cert: DFN-CERT-2024-0773
dfn-cert: DFN-CERT-2024-0750
dfn-cert: DFN-CERT-2024-0730
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0658
dfn-cert: DFN-CERT-2024-0654
dfn-cert: DFN-CERT-2024-0630
dfn-cert: DFN-CERT-2024-0612
dfn-cert: DFN-CERT-2024-0611
dfn-cert: DFN-CERT-2024-0564
dfn-cert: DFN-CERT-2024-0541

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0540
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0505
dfn-cert: DFN-CERT-2024-0504
dfn-cert: DFN-CERT-2024-0503
dfn-cert: DFN-CERT-2024-0488
dfn-cert: DFN-CERT-2024-0487
dfn-cert: DFN-CERT-2024-0486
dfn-cert: DFN-CERT-2024-0457
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-2024-0371
dfn-cert: DFN-CERT-2024-0239
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0142
dfn-cert: DFN-CERT-2024-0123
dfn-cert: DFN-CERT-2024-0121
dfn-cert: DFN-CERT-2024-0095
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0015
dfn-cert: DFN-CERT-2024-0009
dfn-cert: DFN-CERT-2023-3147
dfn-cert: DFN-CERT-2023-3120
dfn-cert: DFN-CERT-2023-3114
dfn-cert: DFN-CERT-2023-3113
dfn-cert: DFN-CERT-2023-3054
dfn-cert: DFN-CERT-2023-2937
dfn-cert: DFN-CERT-2023-2841
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2683
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2580
dfn-cert: DFN-CERT-2023-2579
dfn-cert: DFN-CERT-2023-2578
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0612
dfn-cert: DFN-CERT-2023-0603

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-0602
dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0586
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-0895
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0720
dfn-cert: DFN-CERT-2022-0719
dfn-cert: DFN-CERT-2022-0545
dfn-cert: DFN-CERT-2022-0544
dfn-cert: DFN-CERT-2022-0542
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0540
dfn-cert: DFN-CERT-2022-0433
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6702-1)

Summary
The remote host is missing an update for the 'linux, linux-bluefield, linux-gcp, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-6702-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.174.172
```

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

Affected Software/OS
'linux, linux-bluefield, linux-gcp, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the NVIDIA Tegra XUSB pad controller driver in the Linux kernel did not properly handle return values in certain error conditions. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-23000)

... continues on next page ...

... continued from previous page ...

It was discovered that the ARM Mali Display Processor driver implementation in the Linux kernel did not properly handle certain error conditions. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-23004)
Notselwyn discovered that the netfilter subsystem in the Linux kernel did not properly handle verdict parameters in certain cases, 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-2024-1086)
It was discovered that a race condition existed in the SCSI Emulex LightPulse Fibre Channel driver in the Linux kernel when unregistering FCF and re-scanning an HBA FCF table, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-24855)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6702-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6702.1
Version used: `2024-03-21T04:09:31Z`

References
`url: https://ubuntu.com/security/notices/USN-6702-1`
`cve: CVE-2023-23000`
`cve: CVE-2023-23004`
`cve: CVE-2024-1086`
`cve: CVE-2024-24855`
`advisory_id: USN-6702-1`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0296`
`cert-bund: WID-SEC-2024-0266`
`cert-bund: WID-SEC-2023-0548`
`cert-bund: WID-SEC-2023-0539`
`dfn-cert: DFN-CERT-2024-1455`
`dfn-cert: DFN-CERT-2024-1454`
`dfn-cert: DFN-CERT-2024-1448`
`dfn-cert: DFN-CERT-2024-1427`
`dfn-cert: DFN-CERT-2024-1426`
`dfn-cert: DFN-CERT-2024-1399`
`dfn-cert: DFN-CERT-2024-1309`
`dfn-cert: DFN-CERT-2024-1307`
`dfn-cert: DFN-CERT-2024-1304`
`dfn-cert: DFN-CERT-2024-1249`
`dfn-cert: DFN-CERT-2024-1213`
`dfn-cert: DFN-CERT-2024-1212`
`dfn-cert: DFN-CERT-2024-1207`
`dfn-cert: DFN-CERT-2024-1176`
`dfn-cert: DFN-CERT-2024-1165`
`dfn-cert: DFN-CERT-2024-1068`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1058
dfn-cert: DFN-CERT-2024-1056
dfn-cert: DFN-CERT-2024-1055
dfn-cert: DFN-CERT-2024-0946
dfn-cert: DFN-CERT-2024-0945
dfn-cert: DFN-CERT-2024-0925
dfn-cert: DFN-CERT-2024-0870
dfn-cert: DFN-CERT-2024-0863
dfn-cert: DFN-CERT-2024-0861
dfn-cert: DFN-CERT-2024-0814
dfn-cert: DFN-CERT-2024-0752
dfn-cert: DFN-CERT-2024-0750
dfn-cert: DFN-CERT-2024-0749
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0740
dfn-cert: DFN-CERT-2024-0738
dfn-cert: DFN-CERT-2024-0730
dfn-cert: DFN-CERT-2024-0729
dfn-cert: DFN-CERT-2024-0728
dfn-cert: DFN-CERT-2024-0658
dfn-cert: DFN-CERT-2024-0655
dfn-cert: DFN-CERT-2024-0628
dfn-cert: DFN-CERT-2024-0540
dfn-cert: DFN-CERT-2024-0513
dfn-cert: DFN-CERT-2024-0511
dfn-cert: DFN-CERT-2024-0461
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-2024-0295
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-1923
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1001
dfn-cert: DFN-CERT-2023-0793
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0603
dfn-cert: DFN-CERT-2023-0602

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0601
dfn-cert: DFN-CERT-2023-0586

High (CVSS: 7.6)
NVT: Ubuntu: Security Advisory (USN-5519-1)

Summary
The remote host is missing an update for the 'python2.7, python3.4, python3.5, python3.6, python3.8, python3.9, python3.10' package(s) announced via the USN-5519-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.18-1~20.04.1
Fixed version:      >=python2.7-2.7.18-1~20.04.3
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.18-1~20.04.1
Fixed version:      >=python2.7-minimal-2.7.18-1~20.04.3
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.5
Vulnerable package:   python3.8-minimal
Installed version:    python3.8-minimal-3.8.5-1~20.04.3
Fixed version:      >=python3.8-minimal-3.8.10-0ubuntu1~20.04.5
```

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

Affected Software/OS
'python2.7, python3.4, python3.5, python3.6, python3.8, python3.9, python3.10' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5519-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5519.1
Version used: `2024-02-02T04:09:01Z`

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5519-1
cve: CVE-2015-20107
advisory_id: USN-5519-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0395
cert-bund: WID-SEC-2022-0253
dfn-cert: DFN-CERT-2023-1517
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0552
dfn-cert: DFN-CERT-2022-2572
dfn-cert: DFN-CERT-2022-2264
dfn-cert: DFN-CERT-2022-2184
dfn-cert: DFN-CERT-2022-2020
dfn-cert: DFN-CERT-2022-1537
dfn-cert: DFN-CERT-2022-1307
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6495-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-bluefield, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6495-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.167.164
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-bluefield, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Yu Hao discovered that the UBI driver in the Linux kernel did not properly check for MTD with zero erasesize during device attachment. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-31085)

... continues on next page ...

... continued from previous page ...

Manfred Rudigier discovered that the Intel(R) PCI-Express Gigabit (igb) Ethernet driver in the Linux kernel did not properly validate received frames that are larger than the set MTU size, leading to a buffer overflow vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-45871)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6495-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6495.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-6495-1`
`cve: CVE-2023-31085`
`cve: CVE-2023-45871`
`advisory_id: USN-6495-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2023-2643`
`cert-bund: WID-SEC-2023-1062`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0700`
`dfn-cert: DFN-CERT-2024-0661`
`dfn-cert: DFN-CERT-2024-0655`
`dfn-cert: DFN-CERT-2024-0527`
`dfn-cert: DFN-CERT-2024-0510`
`dfn-cert: DFN-CERT-2024-0481`
`dfn-cert: DFN-CERT-2024-0452`
`dfn-cert: DFN-CERT-2024-0448`
`dfn-cert: DFN-CERT-2024-0281`
`dfn-cert: DFN-CERT-2024-0280`
`dfn-cert: DFN-CERT-2024-0266`
`dfn-cert: DFN-CERT-2024-0250`
`dfn-cert: DFN-CERT-2024-0249`
`dfn-cert: DFN-CERT-2024-0247`
`dfn-cert: DFN-CERT-2024-0213`
`dfn-cert: DFN-CERT-2024-0201`
`dfn-cert: DFN-CERT-2024-0200`
`dfn-cert: DFN-CERT-2024-0143`
`dfn-cert: DFN-CERT-2024-0094`
`dfn-cert: DFN-CERT-2023-3147`
`dfn-cert: DFN-CERT-2023-3123`
`dfn-cert: DFN-CERT-2023-3121`
`dfn-cert: DFN-CERT-2023-3120`
`dfn-cert: DFN-CERT-2023-3118`
`dfn-cert: DFN-CERT-2023-3114`
`dfn-cert: DFN-CERT-2023-3113`
`dfn-cert: DFN-CERT-2023-3054`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-3045
dfn-cert: DFN-CERT-2023-2995
dfn-cert: DFN-CERT-2023-2994
dfn-cert: DFN-CERT-2023-2944
dfn-cert: DFN-CERT-2023-2937
dfn-cert: DFN-CERT-2023-2936
dfn-cert: DFN-CERT-2023-2931
dfn-cert: DFN-CERT-2023-2930
dfn-cert: DFN-CERT-2023-2800
dfn-cert: DFN-CERT-2023-2745
dfn-cert: DFN-CERT-2023-2744
dfn-cert: DFN-CERT-2023-2743
dfn-cert: DFN-CERT-2023-2723
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2721
dfn-cert: DFN-CERT-2023-2720
dfn-cert: DFN-CERT-2023-2719
dfn-cert: DFN-CERT-2023-2718
dfn-cert: DFN-CERT-2023-2683
```

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.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libssl1.1
Installed version:    libssl1.1-1.1.1f-1ubuntu2.4
Fixed version:      >=libssl1.1-1.1.1f-1ubuntu2.17
```

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
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)

... continues on next page ...

... continued from previous page ...

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: `2024-02-02T04:09:01Z`

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-2024-0794`
`cert-bund: WID-SEC-2024-0114`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1886`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1793`
`cert-bund: WID-SEC-2023-1790`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1553
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-0304
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0126
dfn-cert: DFN-CERT-2024-0016
dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1697
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-1043
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0774
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2023-0618
dfn-cert: DFN-CERT-2023-0543
dfn-cert: DFN-CERT-2023-0471
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-6039-1)

Summary
The remote host is missing an update for the 'openssl, openssl1.0' package(s) announced via the USN-6039-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   libssl1.1
Installed version:    libssl1.1-1.1.1f-1ubuntu2.4
Fixed version:      >=libssl1.1-1.1.1f-1ubuntu2.18
Vulnerable package:   openssl
Installed version:    openssl-1.1.1f-1ubuntu2.4
Fixed version:      >=openssl-1.1.1f-1ubuntu2.18
```

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

Affected Software/OS
'openssl, openssl1.0' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that OpenSSL was not properly managing file locks when processing policy constraints. If a user or automated system were tricked into processing a certificate chain with specially crafted policy constraints, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-3996)
David Benjamin discovered that OpenSSL was not properly performing the verification of X.509 certificate chains that include policy constraints, which could lead to excessive resource consumption. If a user or automated system were tricked into processing a specially crafted X.509 certificate chain that includes policy constraints, a remote attacker could possibly use this issue to cause a denial of service. (CVE-2023-0464)
David Benjamin discovered that OpenSSL was not properly handling invalid certificate policies in leaf certificates, which would result in certain policy checks being skipped for the certificate. If a user or automated system were tricked into processing a specially crafted certificate, a remote attacker could possibly use this issue to assert invalid certificate policies and circumvent policy checking. (CVE-2023-0465)
David Benjamin discovered that OpenSSL incorrectly documented the functionalities of function X509_VERIFY_PARAM_add0_policy, stating that it would implicitly enable certificate policy checks when doing certificate verifications, contrary to its implementation. This could cause users and applications to not perform certificate policy checks even when expected to do so. (CVE-2023-0466)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6039-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6039.1
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-6039-1`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-3996
cve: CVE-2023-0464
cve: CVE-2023-0466
advisory_id: USN-6039-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0053
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1781
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2023-1130
cert-bund: WID-SEC-2023-0782
cert-bund: WID-SEC-2023-0732
cert-bund: WID-SEC-2022-2310
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1720
dfn-cert: DFN-CERT-2023-1649
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0999
dfn-cert: DFN-CERT-2023-0960
dfn-cert: DFN-CERT-2023-0782
dfn-cert: DFN-CERT-2023-0700
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0645
dfn-cert: DFN-CERT-2023-0639
dfn-cert: DFN-CERT-2022-2898
dfn-cert: DFN-CERT-2022-2831

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5638-3)

Summary
The remote host is missing an update for the 'expat' package(s) announced via the USN-5638-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libexpat1
Installed version: libexpat1-2.2.9-1build1
Fixed version: >=libexpat1-2.2.9-1ubuntu0.6

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
USN-5638-1 fixed a vulnerability in Expat. This update provides the corresponding updates for Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. (CVE-2022-43680) This update also fixes a minor regression introduced in Ubuntu 18.04 LTS.
We apologize for the inconvenience.
Original advisory details:
Rhodri James discovered that Expat incorrectly handled memory when processing certain malformed XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5638-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5638.3
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5638-3`
`cve: CVE-2022-43680`
`advisory_id: USN-5638-3`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-3226`
`cert-bund: WID-SEC-2023-2676`
`cert-bund: WID-SEC-2023-1818`
`cert-bund: WID-SEC-2023-1807`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-1017`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0292`
`cert-bund: WID-SEC-2023-0132`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-1844`
`dfn-cert: DFN-CERT-2023-3223`
`dfn-cert: DFN-CERT-2023-1651`
`dfn-cert: DFN-CERT-2023-1648`
`dfn-cert: DFN-CERT-2023-1590`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0269
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2821
dfn-cert: DFN-CERT-2022-2566
dfn-cert: DFN-CERT-2022-2480
dfn-cert: DFN-CERT-2022-2408

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6365-1)

Summary
The remote host is missing an update for the 'open-vm-tools' package(s) announced via the USN-6365-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: open-vm-tools
Installed version: open-vm-tools-2:11.2.5-2ubuntu1~ubuntu20.04.1
Fixed version: >=open-vm-tools-2:11.3.0-2ubuntu0~ubuntu20.04.6

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

Affected Software/OS
'open-vm-tools' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Open VM Tools incorrectly handled SAML tokens. A remote attacker could possibly use this issue to bypass SAML token signature verification and perform VMware Tools Guest Operations.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6365-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6365.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6365-1
cve: CVE-2023-20900

... continues on next page ...

... continued from previous page ...

advisory_id: USN-6365-1
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2241
dfn-cert: DFN-CERT-2023-2039
dfn-cert: DFN-CERT-2023-2034

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5328-1)

Summary
The remote host is missing an update for the 'openssl, openssl1.0' package(s) announced via the USN-5328-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssl1.1
Installed version: libssl1.1-1.1.1f-1ubuntu2.4
Fixed version: >=libssl1.1-1.1.1f-1ubuntu2.12

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

Affected Software/OS
'openssl, openssl1.0' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Tavis Ormandy discovered that OpenSSL incorrectly parsed certain certificates. A remote attacker could possibly use this issue to cause OpenSSH to stop responding, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5328-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5328.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5328-1
cve: CVE-2022-0778
advisory_id: USN-5328-1
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1969

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1081
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0551
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0270
cert-bund: WID-SEC-2022-0261
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0190
cert-bund: WID-SEC-2022-0169
cert-bund: WID-SEC-2022-0065
cert-bund: CB-K22/0619
cert-bund: CB-K22/0470
cert-bund: CB-K22/0468
cert-bund: CB-K22/0321
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-0081
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-2111
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1294
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-2022-0955
dfn-cert: DFN-CERT-2022-0902
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0898
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0866
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0779
dfn-cert: DFN-CERT-2022-0759

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0627
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0610
dfn-cert: DFN-CERT-2022-0603

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5546-1)

Summary
The remote host is missing an update for the 'openjdk-8, openjdk-17, openjdk-18, openjdk-lts' package(s) announced via the USN-5546-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.16+8-0ubuntu1~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.16+8-0ubuntu1~20.04
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u342-b07-0ubuntu1~20.04
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u342-b07-0ubuntu1~20.04
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u342-b07-0ubuntu1~20.04
```

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

Affected Software/OS
'openjdk-8, openjdk-17, openjdk-18, openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
Neil Madden discovered that OpenJDK did not properly verify ECDSA signatures. A remote attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 17 and OpenJDK 18. (CVE-2022-21449)

... continues on next page ...

... continued from previous page ...

It was discovered that OpenJDK incorrectly limited memory when compiling a specially crafted XPath expression. An attacker could possibly use this issue to cause a denial of service. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17. (CVE-2022-21426)
It was discovered that OpenJDK incorrectly handled converting certain object arguments into their textual representations. An attacker could possibly use this issue to cause a denial of service. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17. (CVE-2022-21434)
It was discovered that OpenJDK incorrectly validated the encoded length of certain object identifiers. An attacker could possibly use this issue to cause a denial of service. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17. (CVE-2022-21443)
It was discovered that OpenJDK incorrectly validated certain paths. An attacker could possibly use this issue to bypass the secure validation feature and expose sensitive information in XML files. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17. (CVE-2022-21476)
It was discovered that OpenJDK incorrectly parsed certain URI strings. An attacker could possibly use this issue to make applications accept invalid of malformed URI strings. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17. (CVE-2022-21496)
It was discovered that OpenJDK incorrectly generated class code in the Hotspot component. An attacker could possibly use this issue to obtain sensitive information. (CVE-2022-21540)
It was discovered that OpenJDK incorrectly restricted access to the invokeBasic() method in the Hotspot component. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2022-21541)
It was discovered that OpenJDK incorrectly computed exponentials. An attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 17. (CVE-2022-21549)
It was discovered that OpenJDK includes a copy of Xalan that incorrectly handled integer truncation. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-34169)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5546-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5546.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5546-1`
`cve: CVE-2022-21426`
`cve: CVE-2022-21434`
`cve: CVE-2022-21443`
`cve: CVE-2022-21449`
`cve: CVE-2022-21476`
`cve: CVE-2022-21496`
`cve: CVE-2022-21540`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-21541
cve: CVE-2022-21549
cve: CVE-2022-34169
advisory_id: USN-5546-1
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0890
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0788
cert-bund: WID-SEC-2024-0671
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2368
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1032
cert-bund: WID-SEC-2023-1017
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2023-0553
cert-bund: WID-SEC-2023-0122
cert-bund: WID-SEC-2022-1434
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1321
cert-bund: WID-SEC-2022-1244
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1066
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0759
cert-bund: WID-SEC-2022-0746
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0470
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0899
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0819
dfn-cert: DFN-CERT-2023-0082

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2321
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1714
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1607
dfn-cert: DFN-CERT-2022-1606
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0871

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5812-1)

Summary
The remote host is missing an update for the 'python-urllib3' package(s) announced via the USN-5812-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3-urllib3
Installed version: python3-urllib3-1.25.8-2ubuntu0.1
Fixed version: >=python3-urllib3-1.25.8-2ubuntu0.2

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

Affected Software/OS
'python-urllib3' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that urllib3 incorrectly handled certain characters in URLs. A remote attacker could possibly use this issue to cause urllib3 to consume resources, leading to a denial of service.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5812-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5812.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5812-1
cve: CVE-2021-33503
advisory_id: USN-5812-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0156
cert-bund: CB-K21/0954
dfn-cert: DFN-CERT-2021-2428
dfn-cert: DFN-CERT-2021-2354
dfn-cert: DFN-CERT-2021-2353
dfn-cert: DFN-CERT-2021-1930
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1271

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5202-1)

Summary
The remote host is missing an update for the 'openjdk-8, openjdk-lts' package(s) announced via the USN-5202-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.13+8-0ubuntu1~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.13+8-0ubuntu1~20.04
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u312-b07-0ubuntu1~20.04
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u312-b07-0ubuntu1~20.04
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'openjdk-8, openjdk-lts' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
Varnavas Papaioannou discovered that the FTP client implementation in OpenJDK accepted alternate server IP addresses when connecting with FTP passive mode. An attacker controlling an FTP server that an application connects to could possibly use this to expose sensitive information (rudimentary port scans). This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-2341)
Markus Loewe discovered that OpenJDK did not properly handle JAR files containing multiple manifest files. An attacker could possibly use this to bypass JAR signature verification. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-2369)
Huixin Ma discovered that the Hotspot VM in OpenJDK did not properly perform range check elimination in some situations. An attacker could possibly use this to construct a Java class that could bypass Java sandbox restrictions. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. (CVE-2021-2388)
Asaf Greenholts discovered that OpenJDK preferred certain weak ciphers by default. An attacker could possibly use this to expose sensitive information. (CVE-2021-35550)
It was discovered that the Rich Text Format (RTF) Parser in OpenJDK did not properly restrict the amount of memory allocated in some situations. An attacker could use this to specially craft an RTF file that caused a denial of service. (CVE-2021-35556)
It was discovered that the Rich Text Format (RTF) Reader in OpenJDK did not properly restrict the amount of memory allocated in some situations. An attacker could use this to specially craft an RTF file that caused a denial of service. (CVE-2021-35559)
Markus Loewe discovered that the HashMap and HashSet implementations in OpenJDK did not properly validate load factors during deserialization. An attacker could use this to cause a denial of service (excessive memory consumption). (CVE-2021-35561)
It was discovered that the Keytool component in OpenJDK did not properly handle certificates with validity ending dates in the far future. An attacker could use this to specially craft a certificate that when imported could corrupt a keystore. (CVE-2021-35564)
Tristen Hayfield discovered that the HTTP server implementation in OpenJDK did not properly handle TLS session close in some situations. A remote attacker could possibly use this to cause a denial of service (application infinite loop). (CVE-2021-35565)
Chuck Hunley discovered that the Kerberos implementation in OpenJDK did not correctly report subject principals when using Kerberos Constrained Delegation. An attacker could possibly use this to cause incorrect Kerberos tickets to be used. (CVE-2021-35567)
it was discovered that the TLS implementation in OpenJDK did not properly handle TLS handshakes in certain situations where a Java application is acting as a TLS ... [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-5202-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2021.5202.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5202-1
cve: CVE-2021-2341
cve: CVE-2021-2369
cve: CVE-2021-2388
cve: CVE-2021-35550
cve: CVE-2021-35556
cve: CVE-2021-35559
cve: CVE-2021-35561
cve: CVE-2021-35564
cve: CVE-2021-35565
cve: CVE-2021-35567
cve: CVE-2021-35578
cve: CVE-2021-35586
cve: CVE-2021-35588
cve: CVE-2021-35603
advisory_id: USN-5202-1
cert-bund: WID-SEC-2023-0426
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1375
cert-bund: WID-SEC-2022-1162
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0908
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0809
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0677
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0674
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0484
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0464
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0386
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0028

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0024
cert-bund: CB-K22/0675
cert-bund: CB-K22/0310
cert-bund: CB-K22/0239
cert-bund: CB-K21/1082
cert-bund: CB-K21/0981
cert-bund: CB-K21/0783
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2022-1721
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1456
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1247
dfn-cert: DFN-CERT-2022-0580
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0366
dfn-cert: DFN-CERT-2022-0107
dfn-cert: DFN-CERT-2022-0106
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2530
dfn-cert: DFN-CERT-2021-2498
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2310
dfn-cert: DFN-CERT-2021-2195
dfn-cert: DFN-CERT-2021-2194
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1534
dfn-cert: DFN-CERT-2021-1533

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6508-1)

Summary
The remote host is missing an update for the 'poppler' package(s) announced via the USN-6508-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpoppler97
Installed version: libpoppler97-0.86.1-0ubuntu1

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=libpoppler97-0.86.1-0ubuntu1.4
Vulnerable package:   poppler-utils
Installed version:    poppler-utils-0.86.1-0ubuntu1
Fixed version:      >=poppler-utils-0.86.1-0ubuntu1.4
```

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

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

Vulnerability Insight
It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-23804)
It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. (CVE-2022-37050, CVE-2022-37051, CVE-2022-37052, CVE-2022-38349)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6508-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6508.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6508-1
cve: CVE-2020-23804
cve: CVE-2022-37050
cve: CVE-2022-37051
cve: CVE-2022-37052
cve: CVE-2022-38349
advisory_id: USN-6508-1
cert-bund: WID-SEC-2023-2200
cert-bund: WID-SEC-2023-2171
dfn-cert: DFN-CERT-2023-2967
dfn-cert: DFN-CERT-2023-2957
dfn-cert: DFN-CERT-2023-2950
dfn-cert: DFN-CERT-2023-2727
dfn-cert: DFN-CERT-2023-2726
dfn-cert: DFN-CERT-2023-2679
dfn-cert: DFN-CERT-2023-2518
dfn-cert: DFN-CERT-2023-2404
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2403
dfn-cert: DFN-CERT-2023-2376

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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libprotobuf-lite17
Installed version:    libprotobuf-lite17-3.6.1.3-2ubuntu5
Fixed version:      >=libprotobuf-lite17-3.6.1.3-2ubuntu5.2
Vulnerable package:   python3-protobuf
Installed version:    python3-protobuf-3.6.1.3-2ubuntu5
Fixed version:      >=python3-protobuf-3.6.1.3-2ubuntu5.2
```

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: `2024-02-02T04:09:01Z`

... continues on next page ...

... continued from previous page ...

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
cert-bund: WID-SEC-2023-2964
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-2700
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1609
cert-bund: WID-SEC-2023-1016
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-2023-1535
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0874
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-6238-1)

Summary

The remote host is missing an update for the 'samba' package(s) announced via the USN-6238-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: samba

... continues on next page ...

... continued from previous page ...

Installed version: samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version: >=samba-2:4.15.13+dfsg-0ubuntu0.20.04.3

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Samba incorrectly handled Winbind NTLM authentication responses. An attacker could possibly use this issue to cause Samba to crash, resulting in a denial of service. (CVE-2022-2127)
Andreas Schneider discovered that Samba incorrectly enforced SMB2 packet signing. A remote attacker could possibly use this issue to obtain or modify sensitive information. This issue only affected Ubuntu 23.04. (CVE-2023-3347)
Florent Saudel and Arnaud Gatignolof discovered that Samba incorrectly handled certain Spotlight requests. A remote attacker could possibly use this issue to cause Samba to consume resources, leading to a denial of service. (CVE-2023-34966, CVE-2023-34967)
Ralph Boehme and Stefan Metzmacher discovered that Samba incorrectly handled paths returned by Spotlight requests. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-34968)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6238-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6238.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6238-1
cve: CVE-2022-2127
cve: CVE-2023-3347
cve: CVE-2023-34966
cve: CVE-2023-34967
cve: CVE-2023-34968
advisory_id: USN-6238-1
cert-bund: WID-SEC-2023-2910
cert-bund: WID-SEC-2023-1842
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2024-0519
dfn-cert: DFN-CERT-2024-0231
dfn-cert: DFN-CERT-2023-2818
dfn-cert: DFN-CERT-2023-1754

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1744
dfn-cert: DFN-CERT-2023-1741
dfn-cert: DFN-CERT-2023-1666

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6371-1)

Summary
The remote host is missing an update for the 'libssh2' package(s) announced via the USN-6371-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssh2-1
Installed version: libssh2-1-1.8.0-2.1build1
Fixed version: >=libssh2-1-1.8.0-2.1ubuntu0.1

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

Affected Software/OS
'libssh2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that libssh2 incorrectly handled memory access. An attacker could possibly use this issue to cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6371-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6371.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6371-1
cve: CVE-2020-22218
advisory_id: USN-6371-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2023-2177
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2023-2097
dfn-cert: DFN-CERT-2023-2053

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5201-1)

Summary
The remote host is missing an update for the 'python3.8, python3.9' package(s) announced via the USN-5201-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libpython3.8-stdlib
Installed version:    libpython3.8-stdlib-3.8.5-1~20.04.3
Fixed version:      >=libpython3.8-stdlib-3.8.10-0ubuntu1~20.04.2
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.2
Vulnerable package:   python3.8-minimal
Installed version:    python3.8-minimal-3.8.5-1~20.04.3
Fixed version:      >=python3.8-minimal-3.8.10-0ubuntu1~20.04.2
```

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

Affected Software/OS
'python3.8, python3.9' package(s) on Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that the Python urllib http client could enter into an infinite loop when incorrectly handling certain server responses (100 Continue response). Specially crafted traffic from a malicious HTTP server could cause a denial of service (Dos) condition for a client.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5201-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5201.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5201-1
cve: CVE-2021-3737
advisory_id: USN-5201-1
cert-bund: WID-SEC-2023-1524
cert-bund: WID-SEC-2023-0141
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0011
```

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0129
dfn-cert: DFN-CERT-2023-1517
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1056
dfn-cert: DFN-CERT-2022-1053
dfn-cert: DFN-CERT-2022-0972
dfn-cert: DFN-CERT-2022-0968
dfn-cert: DFN-CERT-2022-0235
dfn-cert: DFN-CERT-2021-2649
dfn-cert: DFN-CERT-2021-2648
dfn-cert: DFN-CERT-2021-2353
dfn-cert: DFN-CERT-2021-2207
dfn-cert: DFN-CERT-2021-1956

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6658-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-6658-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libxml2
Installed version: libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version: >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.7

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that libxml2 incorrectly handled certain XML documents. A remote attacker could possibly use this issue to cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6658-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6658.1
Version used: `2024-02-27T04:09:22Z`

References

```
url: https://ubuntu.com/security/notices/USN-6658-1
cve: CVE-2024-25062
advisory_id: USN-6658-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0280
dfn-cert: DFN-CERT-2024-1250
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-0732
dfn-cert: DFN-CERT-2024-0377
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5715-1)

Summary
The remote host is missing an update for the 'libraw' package(s) announced via the USN-5715-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libraw19
Installed version:    libraw19-0.19.5-1ubuntu1
Fixed version:      >=libraw19-0.19.5-1ubuntu1.1
```

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

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

Vulnerability Insight
It was discovered that LibRaw incorrectly handled photo files. If a user or automated system were tricked into processing a specially crafted photo file, a remote attacker could cause applications linked against LibRaw 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-5715-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5715.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5715-1`
`cve: CVE-2020-15503`
`cve: CVE-2020-35530`
`cve: CVE-2020-35531`
`cve: CVE-2020-35532`
`cve: CVE-2020-35533`
`advisory_id: USN-5715-1`
`dfn-cert: DFN-CERT-2022-2490`
`dfn-cert: DFN-CERT-2022-2061`
`dfn-cert: DFN-CERT-2020-2399`
`dfn-cert: DFN-CERT-2020-1436`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5833-1)

Summary
The remote host is missing an update for the 'python-future' package(s) announced via the USN-5833-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-future
Installed version:    python3-future-0.18.2-2
Fixed version:      >=python3-future-0.18.2-2ubuntu0.1
```

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

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

Vulnerability Insight
Sebastian Chnelik discovered that python-future incorrectly handled certain HTTP header field. An attacker could possibly use this issue to cause a denial of service.

... 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-5833-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5833.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5833-1`
`cve: CVE-2022-40899`
`advisory_id: USN-5833-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2229`
`cert-bund: WID-SEC-2023-0089`
`dfn-cert: DFN-CERT-2023-1795`
`dfn-cert: DFN-CERT-2023-0527`
`dfn-cert: DFN-CERT-2023-0087`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5734-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-5734-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libfreerdp-client2-2
Installed version:    libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version:      >=libfreerdp-client2-2-2.2.0+dfsg1-0ubuntu0.20.04.4
```

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

Affected Software/OS
'freerdp2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled certain data lenghts. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive information. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-39282, CVE-2022-39283)

... continues on next page ...

... continued from previous page ...

It was discovered that FreeRDP incorrectly handled certain data lenghts. A malicious server could use this issue to cause FreeRDP clients to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2022-39316, CVE-2022-39317, CVE-2022-39318, CVE-2022-39319, CVE-2022-39320)
It was discovered that FreeRDP incorrectly handled certain path checks. A malicious server could use this issue to cause FreeRDP clients to read files outside of the shared directory. (CVE-2022-39347)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5734-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5734.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5734-1`
`cve: CVE-2022-39282`
`cve: CVE-2022-39283`
`cve: CVE-2022-39316`
`cve: CVE-2022-39317`
`cve: CVE-2022-39318`
`cve: CVE-2022-39319`
`cve: CVE-2022-39320`
`cve: CVE-2022-39347`
`advisory_id: USN-5734-1`
`cert-bund: WID-SEC-2023-1185`
`dfn-cert: DFN-CERT-2023-2897`
`dfn-cert: DFN-CERT-2023-0328`
`dfn-cert: DFN-CERT-2022-2725`
`dfn-cert: DFN-CERT-2022-2687`
`dfn-cert: DFN-CERT-2022-2661`
`dfn-cert: DFN-CERT-2022-2577`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5153-1)

Summary
The remote host is missing an update for the 'libreoffice' package(s) announced via the USN-5153-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libreoffice-core
Installed version:    libreoffice-core-1:6.4.7-0ubuntu0.20.04.1
Fixed version:      >=libreoffice-core-1:6.4.7-0ubuntu0.20.04.2
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'libreoffice' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that LibreOffice incorrectly handled digital signatures. An attacker could possibly use this issue to create a specially crafted document that would display a validly signed indicator, contrary to expectations.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5153-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5153.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5153-1`
`cve: CVE-2021-25633`
`cve: CVE-2021-25634`
`advisory_id: USN-5153-1`
`cert-bund: CB-K21/1051`
`dfn-cert: DFN-CERT-2021-2116`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5330-1)

Summary
The remote host is missing an update for the 'libreoffice' package(s) announced via the USN-5330-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libreoffice-core
Installed version:    libreoffice-core-1:6.4.7-0ubuntu0.20.04.1
Fixed version:      >=libreoffice-core-1:6.4.7-0ubuntu0.20.04.4
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libreoffice' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that LibreOffice incorrectly handled digital signatures. An attacker could possibly use this issue to create a specially crafted document that would display a validly signed indicator, contrary to expectations.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5330-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5330.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5330-1`
`cve: CVE-2021-25636`
`advisory_id: USN-5330-1`
`cert-bund: WID-SEC-2022-1990`
`cert-bund: CB-K22/0226`
`dfn-cert: DFN-CERT-2023-0669`
`dfn-cert: DFN-CERT-2022-0428`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6673-1)

Summary
The remote host is missing an update for the 'python-cryptography' package(s) announced via the USN-6673-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-cryptography
Installed version:    python3-cryptography-2.8-3ubuntu0.1
Fixed version:      >=python3-cryptography-2.8-3ubuntu0.3
```

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

Affected Software/OS
'python-cryptography' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Hubert Kario discovered that python-cryptography incorrectly handled errors returned by the OpenSSL API when processing incorrect padding in RSA PKCS#1 v1.5. A remote attacker could possibly use this issue to expose confidential or sensitive information. (CVE-2023-50782)
It was discovered that python-cryptography incorrectly handled memory operations when processing mismatched PKCS#12 keys. A remote attacker could possibly use this issue to cause python-cryptography to crash, leading to a denial of service. This issue only affected Ubuntu 23.10. (CVE-2024-26130)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6673-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6673.1
Version used: `2024-03-05T04:08:40Z`

References
`url: https://ubuntu.com/security/notices/USN-6673-1`
`cve: CVE-2023-50782`
`cve: CVE-2024-26130`
`advisory_id: USN-6673-1`
`cert-bund: WID-SEC-2024-1328`
`cert-bund: WID-SEC-2024-0869`
`dfn-cert: DFN-CERT-2024-0905`
`dfn-cert: DFN-CERT-2024-0575`
`dfn-cert: DFN-CERT-2024-0566`
`dfn-cert: DFN-CERT-2024-0524`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6233-2)

Summary
The remote host is missing an update for the 'yajl' package(s) announced via the USN-6233-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libyajl2
Installed version:    libyajl2-2.1.0-3
Fixed version:      >=libyajl2-2.1.0-3ubuntu0.20.04.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'yajl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
USN-6233-1 fixed vulnerabilities in YAJL. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04.
Original advisory details:
It was discovered that YAJL was not properly performing bounds checks when decoding a string with escape sequences. If a user or automated system using YAJL were tricked into processing specially crafted input, an attacker could possibly use this issue to cause a denial of service (application abort). (CVE-2017-16516)
It was discovered that YAJL was not properly handling memory allocation when dealing with large inputs, which could lead to heap memory corruption. If a user or automated system using YAJL were tricked into running a specially crafted large input, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-24795)
It was discovered that memory leaks existed in one of the YAJL parsing functions. An attacker could possibly use this issue to cause a denial of service (memory exhaustion). (CVE-2023-33460)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6233-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6233.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6233-2`
`cve: CVE-2017-16516`
`cve: CVE-2022-24795`
`cve: CVE-2023-33460`
`advisory_id: USN-6233-2`
`cert-bund: WID-SEC-2023-2853`
`cert-bund: WID-SEC-2022-0067`
`dfn-cert: DFN-CERT-2023-1593`
`dfn-cert: DFN-CERT-2023-1575`
`dfn-cert: DFN-CERT-2023-1518`
`dfn-cert: DFN-CERT-2022-0792`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6539-1)

Summary
The remote host is missing an update for the 'python-cryptography' package(s) announced via the USN-6539-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package:   python3-cryptography
Installed version:    python3-cryptography-2.8-3ubuntu0.1
Fixed version:      >=python3-cryptography-2.8-3ubuntu0.2
```

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

Affected Software/OS
'python-cryptography' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that the python-cryptography Cipher.update_into function would incorrectly accept objects with immutable buffers. This would result in corrupted output, contrary to expectations. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-23931)
It was dicovered that python-cryptography incorrectly handled loading certain PKCS7 certificates. A remote attacker could possibly use this issue to cause python-cryptography to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-49083)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6539-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6539.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6539-1
cve: CVE-2023-23931
cve: CVE-2023-49083
advisory_id: USN-6539-1
cert-bund: WID-SEC-2024-1328
cert-bund: WID-SEC-2024-0995
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-2922
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2266
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1818
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1793
cert-bund: WID-SEC-2023-1021
dfn-cert: DFN-CERT-2024-1391
dfn-cert: DFN-CERT-2024-0312
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0174
dfn-cert: DFN-CERT-2023-3146
dfn-cert: DFN-CERT-2023-3056
dfn-cert: DFN-CERT-2023-3014
dfn-cert: DFN-CERT-2023-2783
dfn-cert: DFN-CERT-2023-1656
dfn-cert: DFN-CERT-2023-1651
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0440

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6717-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6717-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: thunderbird
Installed version: thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version: >=thunderbird-1:115.9.0+build1-0ubuntu0.20.04.1

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

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

Vulnerability Insight
Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-0743, CVE-2024-2611, CVE-2024-2614)
Hubert Kario discovered that Thunderbird had a timing side-channel when performing RSA decryption. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2023-5388)
Gary Kwong discovered that Thunderbird incorrectly updated return registers for JIT code on Armv7-A systems. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2024-2607)

... continues on next page ...

... continued from previous page ...

Ronald Crane discovered that Thunderbird did not properly manage memory during character encoding. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2608)
Georg Felber and Marco Squarcina discovered that Thunderbird incorrectly handled html and body tags. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able obtain sensitive information. (CVE-2024-2610)
Ronald Crane discovered a use-after-free in Thunderbird when handling code in SafeRefPtr. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-2612)
Ryan VanderMeulen and Dan Minor discovered that Thunderbird did not properly manage memory conditions in ICU. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2616)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6717-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6717.1
Version used: `2024-03-27T04:09:51Z`

References
`url: https://ubuntu.com/security/notices/USN-6717-1`
`cve: CVE-2023-5388`
`cve: CVE-2024-0743`
`cve: CVE-2024-2607`
`cve: CVE-2024-2608`
`cve: CVE-2024-2610`
`cve: CVE-2024-2611`
`cve: CVE-2024-2612`
`cve: CVE-2024-2614`
`cve: CVE-2024-2616`
`advisory_id: USN-6717-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0669`
`cert-bund: WID-SEC-2024-0185`
`cert-bund: WID-SEC-2024-0045`
`dfn-cert: DFN-CERT-2024-1071`
`dfn-cert: DFN-CERT-2024-1011`
`dfn-cert: DFN-CERT-2024-0955`
`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-2024-0188`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0069

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5821-3)

Summary
The remote host is missing an update for the 'python-pip' package(s) announced via the USN-5821-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python-pip-whl
Installed version:    python-pip-whl-20.0.2-5ubuntu1.5
Fixed version:      >=python-pip-whl-20.0.2-5ubuntu1.8
Vulnerable package:   python3-pip
Installed version:    python3-pip-20.0.2-5ubuntu1.5
Fixed version:      >=python3-pip-20.0.2-5ubuntu1.8
```

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

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

Vulnerability Insight
USN-5821-1 fixed a vulnerability in wheel and pip. Unfortunately, it was missing a commit to fix it properly in pip.
We apologize for the inconvenience.
Original advisory details:
Sebastian Chnelik discovered that wheel incorrectly handled certain file names when validated against a regex expression. 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-5821-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5821.3
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5821-3
cve: CVE-2022-40898
advisory_id: USN-5821-3
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2853
cert-bund: WID-SEC-2023-1424
dfn-cert: DFN-CERT-2023-2783
dfn-cert: DFN-CERT-2023-0718
dfn-cert: DFN-CERT-2023-0101

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5412-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5412-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.11
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.11
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.11
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Axel Chong discovered that curl incorrectly handled percent-encoded URL separators. A remote attacker could possibly use this issue to trick curl into using the wrong URL and bypass certain checks or filters. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-27780)
Florian Kohnhuser discovered that curl incorrectly handled returning a TLS server's certificate chain details. A remote attacker could possibly use this issue to cause curl to stop responding, resulting in a denial of service. (CVE-2022-27781)
Harry Sintonen discovered that curl incorrectly reused a previous connection when certain options had been changed, contrary to expectations. (CVE-2022-27782)

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-5412-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5412.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5412-1
cve: CVE-2022-27780
cve: CVE-2022-27781
cve: CVE-2022-27782
advisory_id: USN-5412-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2023-0125
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1145
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0277
cert-bund: CB-K22/0570
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-0122
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2086
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1830
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1464
dfn-cert: DFN-CERT-2022-1454
dfn-cert: DFN-CERT-2022-1140
dfn-cert: DFN-CERT-2022-1049

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5716-1)

Summary

The remote host is missing an update for the 'sqlite3' package(s) announced via the USN-5716-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: libsqlite3-0
Installed version: libsqlite3-0-3.31.1-4ubuntu0.2
Fixed version: >=libsqlite3-0-3.31.1-4ubuntu0.5

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

Affected Software/OS
'sqlite3' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that SQLite incorrectly handled certain long string arguments. An attacker could use this issue to cause SQLite to crash, resulting in 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-5716-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5716.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5716-1
cve: CVE-2022-35737
advisory_id: USN-5716-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0036
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0419
cert-bund: WID-SEC-2023-0138
cert-bund: WID-SEC-2022-2290
cert-bund: WID-SEC-2022-1972
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1766
dfn-cert: DFN-CERT-2024-0229
dfn-cert: DFN-CERT-2024-0055
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2022-2472
dfn-cert: DFN-CERT-2022-2306

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2079

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6463-1)

Summary
The remote host is missing an update for the 'open-vm-tools' package(s) announced via the USN-6463-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   open-vm-tools
Installed version:    open-vm-tools-2:11.2.5-2ubuntu1~ubuntu20.04.1
Fixed version:      >=open-vm-tools-2:11.3.0-2ubuntu0~ubuntu20.04.7
Vulnerable package:   open-vm-tools-desktop
Installed version:    open-vm-tools-desktop-2:11.2.5-2ubuntu1~ubuntu20.04.1
Fixed version:      >=open-vm-tools-desktop-2:11.3.0-2ubuntu0~ubuntu20.04.7
```

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

Affected Software/OS
'open-vm-tools' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that Open VM Tools incorrectly handled SAML tokens. A remote attacker Guest Operations privileges could possibly use this issue to escalate privileges. (CVE-2023-34058) Matthias Gerstner discovered that Open VM Tools incorrectly handled file descriptors when dropping privileges. A local attacker could possibly use this issue to hijack /dev/uinput and simulate user inputs. (CVE-2023-34059)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6463-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6463.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6463-1
cve: CVE-2023-34058
cve: CVE-2023-34059
advisory_id: USN-6463-1
cert-bund: WID-SEC-2024-1092
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2756
dfn-cert: DFN-CERT-2023-2659
dfn-cert: DFN-CERT-2023-2647

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5514-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5514-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.122.123

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gke, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1195)
Duoming Zhou discovered that the AX.25 amateur radio protocol implementation in the Linux kernel did not handle detach events properly in some situations. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2022-1199)
Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel during device detach operations. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1204)
Duoming Zhou discovered race conditions in the AX.25 amateur radio protocol implementation in the Linux kernel, leading to use-after-free vulnerabilities. A local attacker could possibly use this to cause a denial of service (system crash). (CVE-2022-1205)

... continues on next page ...

... continued from previous page ...

Yongkang Jia discovered that the KVM hypervisor implementation in the Linux kernel did not properly handle guest TLB mapping invalidation requests in some situations. An attacker in a guest VM could use this to cause a denial of service (system crash) in the host OS. (CVE-2022-1789)
Minh Yuan discovered that the floppy driver in the Linux kernel contained a race condition in some situations, 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-2022-33981)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5514-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5514.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5514-1`
`cve: CVE-2022-1195`
`cve: CVE-2022-1199`
`cve: CVE-2022-1204`
`cve: CVE-2022-1205`
`cve: CVE-2022-1789`
`cve: CVE-2022-33981`
`advisory_id: USN-5514-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-0412`
`cert-bund: WID-SEC-2022-0268`
`cert-bund: WID-SEC-2022-0162`
`cert-bund: WID-SEC-2022-0161`
`cert-bund: CB-K22/0658`
`cert-bund: CB-K22/0387`
`cert-bund: CB-K22/0383`
`dfn-cert: DFN-CERT-2023-1116`
`dfn-cert: DFN-CERT-2023-1041`
`dfn-cert: DFN-CERT-2023-0866`
`dfn-cert: DFN-CERT-2023-0861`
`dfn-cert: DFN-CERT-2023-0376`
`dfn-cert: DFN-CERT-2022-2915`
`dfn-cert: DFN-CERT-2022-2891`
`dfn-cert: DFN-CERT-2022-2646`
`dfn-cert: DFN-CERT-2022-2599`
`dfn-cert: DFN-CERT-2022-2174`
`dfn-cert: DFN-CERT-2022-1823`
`dfn-cert: DFN-CERT-2022-1802`
`dfn-cert: DFN-CERT-2022-1794`
`dfn-cert: DFN-CERT-2022-1707`
`dfn-cert: DFN-CERT-2022-1677`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1675
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1598
dfn-cert: DFN-CERT-2022-1592
dfn-cert: DFN-CERT-2022-1586
dfn-cert: DFN-CERT-2022-1579
dfn-cert: DFN-CERT-2022-1577
dfn-cert: DFN-CERT-2022-1576
dfn-cert: DFN-CERT-2022-1570
dfn-cert: DFN-CERT-2022-1565
dfn-cert: DFN-CERT-2022-1564
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1312
dfn-cert: DFN-CERT-2022-1279
dfn-cert: DFN-CERT-2022-1278
dfn-cert: DFN-CERT-2022-1238
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0910
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0790
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5179-1)

Summary
The remote host is missing an update for the 'busybox' package(s) announced via the USN-5179-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   busybox-initramfs
Installed version:    busybox-initramfs-1:1.30.1-4ubuntu6.3
Fixed version:      >=busybox-initramfs-1:1.30.1-4ubuntu6.4
Vulnerable package:   busybox-static
Installed version:    busybox-static-1:1.30.1-4ubuntu6.3
Fixed version:      >=busybox-static-1:1.30.1-4ubuntu6.4
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'busybox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that BusyBox incorrectly handled certain malformed gzip archives. If a user or automated system were tricked into processing a specially crafted gzip archive, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-28831)
It was discovered that BusyBox incorrectly handled certain malformed LZMA archives. If a user or automated system were tricked into processing a specially crafted LZMA archive, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly leak sensitive information. (CVE-2021-42374)
Vera Mens, Uri Katz, Tal Keren, Sharon Brizinov, and Shachar Menashe discovered that BusyBox incorrectly handled certain awk patterns. If a user or automated system were tricked into processing a specially crafted awk pattern, a remote attacker could use this issue to cause BusyBox to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5179-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5179.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5179-1`
`cve: CVE-2021-28831`
`cve: CVE-2021-42374`
`cve: CVE-2021-42378`
`cve: CVE-2021-42379`
`cve: CVE-2021-42380`
`cve: CVE-2021-42381`
`cve: CVE-2021-42382`
`cve: CVE-2021-42384`
`cve: CVE-2021-42385`
`cve: CVE-2021-42386`
`advisory_id: USN-5179-1`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2022-2029`
`cert-bund: WID-SEC-2022-2028`
`dfn-cert: DFN-CERT-2023-2049`
`dfn-cert: DFN-CERT-2022-2699`
`dfn-cert: DFN-CERT-2022-0148`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-2550
dfn-cert: DFN-CERT-2021-2430
dfn-cert: DFN-CERT-2021-2247
dfn-cert: DFN-CERT-2021-0604

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5342-2)

Summary
The remote host is missing an update for the 'python2.7' package(s) announced via the USN-5342-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.18-1~20.04.1
Fixed version:      >=python2.7-2.7.18-1~20.04.3+esm1
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.18-1~20.04.1
Fixed version:      >=python2.7-minimal-2.7.18-1~20.04.3+esm1
```

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

Affected Software/OS
'python2.7' package(s) on Ubuntu 14.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
USN-5342-1 fixed several vulnerabilities in Python. This update provides the corresponding update for Ubuntu 14.04 ESM, Ubuntu 20.04 ESM and Ubuntu 22.04 ESM.
Original advisory details:
It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. (CVE-2021-4189)
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-0391)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5342-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5342.2
Version used: `2024-02-02T04:09:01Z`

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5342-2
cve: CVE-2021-4189
cve: CVE-2022-0391
advisory_id: USN-5342-2
cert-bund: WID-SEC-2023-0831
cert-bund: WID-SEC-2023-0426
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0146
cert-bund: WID-SEC-2022-0011
cert-bund: CB-K22/0310
dfn-cert: DFN-CERT-2023-2237
dfn-cert: DFN-CERT-2023-2227
dfn-cert: DFN-CERT-2023-1517
dfn-cert: DFN-CERT-2023-1472
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2022-2020
dfn-cert: DFN-CERT-2022-1304
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1056
dfn-cert: DFN-CERT-2022-1053
dfn-cert: DFN-CERT-2022-0968
dfn-cert: DFN-CERT-2022-0865
dfn-cert: DFN-CERT-2022-0742
dfn-cert: DFN-CERT-2022-0690
dfn-cert: DFN-CERT-2022-0618
dfn-cert: DFN-CERT-2022-0577
dfn-cert: DFN-CERT-2022-0576
dfn-cert: DFN-CERT-2022-0351
dfn-cert: DFN-CERT-2022-0223
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5372-1)

Summary
The remote host is missing an update for the 'subversion' package(s) announced via the USN-5372-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libsvn1
Installed version:    libsvn1-1.13.0-3
Fixed version:      >=libsvn1-1.13.0-3ubuntu0.1
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'subversion' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Evgeny Kotkov discovered that Subversion servers did not properly follow path-based authorization rules in certain cases. An attacker could potentially use this issue to retrieve information about private paths. (CVE-2021-28544)
Thomas Weissschuh discovered that Subversion servers did not properly handle memory in certain configurations. A remote attacker could potentially use this issue to cause a denial of service or other unspecified impact. (CVE-2022-24070)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5372-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5372.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5372-1`
`cve: CVE-2021-28544`
`cve: CVE-2022-24070`
`advisory_id: USN-5372-1`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-0778`
`cert-bund: WID-SEC-2022-0199`
`cert-bund: CB-K22/0436`
`dfn-cert: DFN-CERT-2022-2601`
`dfn-cert: DFN-CERT-2022-1633`
`dfn-cert: DFN-CERT-2022-1083`
`dfn-cert: DFN-CERT-2022-0991`
`dfn-cert: DFN-CERT-2022-0818`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5445-1)

Summary
The remote host is missing an update for the 'subversion' package(s) announced via the USN-5445-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: libsvn1
Installed version: libsvn1-1.13.0-3
Fixed version: >=libsvn1-1.13.0-3ubuntu0.2

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

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

Vulnerability Insight
Ace Olszowka discovered that Subversion incorrectly handled certain svnserve requests. A remote attacker could possibly use this issue to cause svnserver to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-11782)
Tomas Bortoli discovered that Subversion incorrectly handled certain svnserve requests. A remote attacker could possibly use this issue to cause svnserver to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2019-0203)
Thomas Akesson discovered that Subversion incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-17525)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5445-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5445.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5445-1
cve: CVE-2018-11782
cve: CVE-2019-0203
cve: CVE-2020-17525
advisory_id: USN-5445-1
cert-bund: CB-K21/0174
cert-bund: CB-K20/1030
cert-bund: CB-K19/0680
dfn-cert: DFN-CERT-2022-1198
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0308
dfn-cert: DFN-CERT-2020-2388
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-1566

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5788-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5788-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.15
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.15
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.15
```

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
Hiroki Kurosawa discovered that curl incorrectly handled HSTS support when certain hostnames included IDN characters. 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-2022-43551)
It was discovered that curl incorrectly handled denials when using HTTP proxies. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-43552)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5788-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5788.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5788-1
cve: CVE-2022-43551
cve: CVE-2022-43552
advisory_id: USN-5788-1
```

. . . continues on next page . . .

... continued from previous page ...

cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-1033
cert-bund: WID-SEC-2023-1016
cert-bund: WID-SEC-2023-0777
cert-bund: WID-SEC-2022-2375
dfn-cert: DFN-CERT-2024-0230
dfn-cert: DFN-CERT-2023-1522
dfn-cert: DFN-CERT-2023-1423
dfn-cert: DFN-CERT-2023-1297
dfn-cert: DFN-CERT-2023-1141
dfn-cert: DFN-CERT-2023-1044
dfn-cert: DFN-CERT-2023-0898
dfn-cert: DFN-CERT-2023-0885
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0685
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0363
dfn-cert: DFN-CERT-2023-0216
dfn-cert: DFN-CERT-2023-0214
dfn-cert: DFN-CERT-2022-2903
dfn-cert: DFN-CERT-2022-2902

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5359-1)

Summary
The remote host is missing an update for the 'rsync' package(s) announced via the USN-5359-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: rsync
Installed version: rsync-3.1.3-8
Fixed version: >=rsync-3.1.3-8ubuntu0.3

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
Danilo Ramos discovered that rsync incorrectly handled memory when performing certain zlib deflating operations. An attacker could use this issue to cause rsync to crash, resulting in 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-5359-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5359.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5359-1`
`cve: CVE-2018-25032`
`advisory_id: USN-5359-1`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1784`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-0141`
`cert-bund: WID-SEC-2023-0132`
`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-2022-0767`
`cert-bund: WID-SEC-2022-0736`
`cert-bund: WID-SEC-2022-0735`
`cert-bund: WID-SEC-2022-0677`
`cert-bund: WID-SEC-2022-0554`
`cert-bund: WID-SEC-2022-0005`
`cert-bund: CB-K22/0619`
`cert-bund: CB-K22/0386`
`dfn-cert: DFN-CERT-2024-0998`
`dfn-cert: DFN-CERT-2024-0790`
`dfn-cert: DFN-CERT-2023-3028`
`dfn-cert: DFN-CERT-2023-0553`
`dfn-cert: DFN-CERT-2023-0430`
`dfn-cert: DFN-CERT-2023-0121`
`dfn-cert: DFN-CERT-2023-0119`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2668
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
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

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5619-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5619-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.5

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

It was discovered that LibTIFF was not properly performing the calculation of data that would eventually be used as a reference for bound-checking operations. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-19131)

It was discovered that LibTIFF was not properly terminating a function execution when processing incorrect data. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-19144)

It was discovered that LibTIFF did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted TIFF file using tiffinfo tool, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-1354)

It was discovered that LibTIFF did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted TIFF file using tiffcp tool, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-1355)

It was discovered that LibTIFF was not properly performing checks to avoid division calculations where the denominator value was zero, which could lead to an undefined behaviour situation via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2056, CVE-2022-2057, CVE-2022-2058)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5619-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5619.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5619-1`
`cve: CVE-2020-19131`
`cve: CVE-2020-19144`
`cve: CVE-2022-1354`
`cve: CVE-2022-1355`
`cve: CVE-2022-2056`
`cve: CVE-2022-2057`
`cve: CVE-2022-2058`
`advisory_id: USN-5619-1`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-1250`
`cert-bund: WID-SEC-2022-0723`
`cert-bund: WID-SEC-2022-0544`
`cert-bund: WID-SEC-2022-0220`
`dfn-cert: DFN-CERT-2023-0218`
`dfn-cert: DFN-CERT-2023-0165`
`dfn-cert: DFN-CERT-2023-0141`
`dfn-cert: DFN-CERT-2023-0084`
`dfn-cert: DFN-CERT-2022-2601`
`dfn-cert: DFN-CERT-2022-2592`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2494
dfn-cert: DFN-CERT-2022-2089
dfn-cert: DFN-CERT-2022-1601
dfn-cert: DFN-CERT-2022-1505
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1259
dfn-cert: DFN-CERT-2022-1061
dfn-cert: DFN-CERT-2022-0389
dfn-cert: DFN-CERT-2021-2100

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5672-1)

Summary
The remote host is missing an update for the 'gmp' package(s) announced via the USN-5672-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgmp10
Installed version: libgmp10-2:6.2.0+dfsg-4
Fixed version: >=libgmp10-2:6.2.0+dfsg-4ubuntu0.1

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

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

Vulnerability Insight
It was discovered that GMP did not properly manage memory on 32-bit platforms when processing a specially crafted input. An attacker could possibly use this issue to cause applications using GMP to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5672-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5672.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5672-1
cve: CVE-2021-43618

... continues on next page ...

... continued from previous page ...

```
advisory_id: USN-5672-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2023-2853
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2022-2024
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2021-2518
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5550-1)

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-5550-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgnutls30
Installed version:    libgnutls30-3.6.13-2ubuntu1.3
Fixed version:      >=libgnutls30-3.6.13-2ubuntu1.7
```

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

Affected Software/OS
'gnutls28' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that GnuTLS incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2021-4209)
It was discovered that GnuTLS incorrectly handled the verification of certain pkcs7 signatures. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-2509)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5550-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5550.1
Version used: `2024-02-02T04:09:01Z`

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-5550-1
cve: CVE-2021-4209
cve: CVE-2022-2509
advisory_id: USN-5550-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-0920
cert-bund: WID-SEC-2022-0872
cert-bund: CB-K22/0256
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-1737
dfn-cert: DFN-CERT-2022-1684
dfn-cert: DFN-CERT-2022-0484

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: git
Installed version: git-1:2.25.1-1ubuntu3.1
Fixed version: >=git-1:2.25.1-1ubuntu3.10

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)

... 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-5871-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5871.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5871-1`
`cve: CVE-2023-22490`
`cve: CVE-2023-23946`
`advisory_id: USN-5871-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0641`
`cert-bund: WID-SEC-2023-0371`
`dfn-cert: DFN-CERT-2024-0228`
`dfn-cert: DFN-CERT-2023-1177`
`dfn-cert: DFN-CERT-2023-0884`
`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-6593-1)

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-6593-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libgnutls30
Installed version:    libgnutls30-3.6.13-2ubuntu1.3
Fixed version:      >=libgnutls30-3.6.13-2ubuntu1.10
```

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

Affected Software/OS
'gnutls28' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that GnuTLS had a timing side-channel when processing malformed ciphertexts in RSA-PSK ClientKeyExchange. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2024-0553)
It was discovered that GnuTLS incorrectly handled certain certificate chains with a cross-signing loop. 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, Ubuntu 23.04, and Ubuntu 23.10. (CVE-2024-0567)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6593-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6593.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6593-1`
`cve: CVE-2024-0553`
`cve: CVE-2024-0567`
`advisory_id: USN-6593-1`
`cert-bund: WID-SEC-2024-0521`
`cert-bund: WID-SEC-2024-0131`
`dfn-cert: DFN-CERT-2024-1072`
`dfn-cert: DFN-CERT-2024-0940`
`dfn-cert: DFN-CERT-2024-0744`
`dfn-cert: DFN-CERT-2024-0539`
`dfn-cert: DFN-CERT-2024-0496`
`dfn-cert: DFN-CERT-2024-0309`
`dfn-cert: DFN-CERT-2024-0205`
`dfn-cert: DFN-CERT-2024-0137`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6263-1)

Summary
The remote host is missing an update for the 'openjdk-8, openjdk-17, openjdk-lts' package(s) announced via the USN-6263-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.20+8-1ubuntu1~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.20+8-1ubuntu1~20.04
```

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u382-ga-1~20.04.1
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u382-ga-1~20.04.1
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u382-ga-1~20.04.1
```

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

Affected Software/OS
'openjdk-8, openjdk-17, openjdk-lts' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Motoyasu Saburi discovered that OpenJDK incorrectly handled special characters in file name parameters. An attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22006)
Eirik Bjorsnos discovered that OpenJDK incorrectly handled certain ZIP archives. An attacker could possibly use this issue to cause a denial of service. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22036)
David Stancu discovered that OpenJDK had a flaw in the AES cipher implementation. An attacker could possibly use this issue to obtain sensitive information. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22041)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array accesses when using the binary '%' operator. An attacker could possibly use this issue to obtain sensitive information. This issue only affected OpenJDK 17. (CVE-2023-22044)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array accesses. An attacker could possibly use this issue to obtain sensitive information. (CVE-2023-22045)
It was discovered that OpenJDK incorrectly sanitized URIs strings. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-22049)
It was discovered that OpenJDK incorrectly handled certain glyphs. An attacker could possibly use this issue to cause a denial of service. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-25193)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6263-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6263.1
Version used: `2024-02-02T04:09:01Z`

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6263-1
cve: CVE-2023-22006
cve: CVE-2023-22036
cve: CVE-2023-22041
cve: CVE-2023-22044
cve: CVE-2023-22045
cve: CVE-2023-22049
cve: CVE-2023-25193
advisory_id: USN-6263-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-3167
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-2042
dfn-cert: DFN-CERT-2023-2031
dfn-cert: DFN-CERT-2023-1990
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1935
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
dfn-cert: DFN-CERT-2023-1304
dfn-cert: DFN-CERT-2023-0850
dfn-cert: DFN-CERT-2023-0316
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6139-1)

Summary
The remote host is missing an update for the 'python2.7, python3.5, python3.6, python3.8, python3.10, python3.11' package(s) announced via the USN-6139-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.8
```

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'python2.7, python3.5, python3.6, python3.8, python3.10, python3.11' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Yebo Cao discovered that Python incorrectly handled certain URLs. An attacker could use this issue to bypass blockinglisting methods. This issue was first addressed in USN-5960-1, but was incomplete. Here we address an additional fix to that issue. (CVE-2023-24329)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6139-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6139.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6139-1`
`cve: CVE-2023-24329`
`advisory_id: USN-6139-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2964`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-0513`
`dfn-cert: DFN-CERT-2023-2783`
`dfn-cert: DFN-CERT-2023-2542`
`dfn-cert: DFN-CERT-2023-2237`
`dfn-cert: DFN-CERT-2023-2227`
`dfn-cert: DFN-CERT-2023-1728`
`dfn-cert: DFN-CERT-2023-1667`
`dfn-cert: DFN-CERT-2023-1472`
`dfn-cert: DFN-CERT-2023-0571`
`dfn-cert: DFN-CERT-2023-0552`
`dfn-cert: DFN-CERT-2023-0527`
`dfn-cert: DFN-CERT-2023-0525`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6263-2)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'openjdk-17, openjdk-lts' package(s) announced via the USN-6263-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.20.1+1-0ubuntu1~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.20.1+1-0ubuntu1~20.04
```

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

Affected Software/OS
'openjdk-17, openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
USN-6263-1 fixed vulnerabilities in OpenJDK. Unfortunately, that update introduced a regression when opening APK, ZIP or JAR files in OpenJDK 11 and OpenJDK 17. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
Motoyasu Saburi discovered that OpenJDK incorrectly handled special characters in file name parameters. An attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22006)
Eirik Bjorsnos discovered that OpenJDK incorrectly handled certain ZIP archives. An attacker could possibly use this issue to cause a denial of service. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22036)
David Stancu discovered that OpenJDK had a flaw in the AES cipher implementation. An attacker could possibly use this issue to obtain sensitive information. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-22041)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array accesses when using the binary '%' operator. An attacker could possibly use this issue to obtain sensitive information. This issue only affected OpenJDK 17. (CVE-2023-22044)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array accesses. An attacker could possibly use this issue to obtain sensitive information. (CVE-2023-22045)
It was discovered that OpenJDK incorrectly sanitized URIs strings. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-22049)
It was discovered that OpenJDK incorrectly handled certain glyphs. An attacker could possibly use this issue to cause a denial of service. This issue only affected OpenJDK 11 and OpenJDK 17. (CVE-2023-25193)

... 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-6263-2)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6263.2
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6263-2
url: https://launchpad.net/bugs/2032865
cve: CVE-2023-22006
cve: CVE-2023-22036
cve: CVE-2023-22041
cve: CVE-2023-22044
cve: CVE-2023-22045
cve: CVE-2023-22049
cve: CVE-2023-25193
advisory_id: USN-6263-2
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1814
cert-bund: WID-SEC-2023-1796
dfn-cert: DFN-CERT-2023-3167
dfn-cert: DFN-CERT-2023-2179
dfn-cert: DFN-CERT-2023-2042
dfn-cert: DFN-CERT-2023-2031
dfn-cert: DFN-CERT-2023-1990
dfn-cert: DFN-CERT-2023-1972
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1935
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1657
dfn-cert: DFN-CERT-2023-1653
dfn-cert: DFN-CERT-2023-1304
dfn-cert: DFN-CERT-2023-0850
dfn-cert: DFN-CERT-2023-0316

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5675-1)

Summary
The remote host is missing an update for the 'heimdal' package(s) announced via the USN-5675-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1.1
Vulnerable package:   libkrb5-26-heimdal
Installed version:    libkrb5-26-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libkrb5-26-heimdal-7.7.0+dfsg-1ubuntu1.1
```

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

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

Vulnerability Insight
Isaac Boukris and Andrew Bartlett discovered that Heimdal's KDC was not properly performing checksum algorithm verifications in the S4U2Self extension module. An attacker could possibly use this issue to perform a machine-in-the-middle attack and request S4U2Self tickets for any user known by the application. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2018-16860)
It was discovered that Heimdal was not properly handling the verification of key exchanges when an anonymous PKINIT was being used. An attacker could possibly use this issue to perform a machine-in-the-middle attack and expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2019-12098)
Joseph Sutton discovered that Heimdal was not properly handling memory management operations when dealing with TGS-REQ tickets that were missing information. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-3671)
Michal Kepien discovered that Heimdal was not properly handling logical conditions that related to memory management operations. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-3116)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5675-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5675.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5675-1
cve: CVE-2018-16860
cve: CVE-2019-12098
cve: CVE-2021-3671
```

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-3116
advisory_id: USN-5675-1
cert-bund: WID-SEC-2023-0781
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1714
cert-bund: WID-SEC-2022-1713
cert-bund: WID-SEC-2022-1712
cert-bund: CB-K21/1034
cert-bund: CB-K19/0649
cert-bund: CB-K19/0644
cert-bund: CB-K19/0396
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2269
dfn-cert: DFN-CERT-2021-2539
dfn-cert: DFN-CERT-2019-1512
dfn-cert: DFN-CERT-2019-1511
dfn-cert: DFN-CERT-2019-1124
dfn-cert: DFN-CERT-2019-0955
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5849-1)

Summary
The remote host is missing an update for the 'heimdal' package(s) announced via the USN-5849-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libgssapi3-heimdal-7.7.0+dfsg-1ubuntu1.4
```

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

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

Vulnerability Insight
Helmut Grohne discovered that Heimdal GSSAPI incorrectly handled logical conditions that are related to memory management operations. An attacker could possibly use this issue to cause a denial of service.

... 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-5849-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5849.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5849-1`
`cve: CVE-2022-45142`
`advisory_id: USN-5849-1`
`cert-bund: WID-SEC-2023-0310`
`dfn-cert: DFN-CERT-2023-0293`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6644-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-6644-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version:      >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.12
```

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 23.10.

Vulnerability Insight
It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause the application to crash, resulting in a denial of service. (CVE-2023-52356)
It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-6228)
It was discovered that LibTIFF incorrectly handled certain files. If a user were tricked into opening a specially crafted file, an attacker could possibly use this issue to consume resources, resulting in a denial of service. (CVE-2023-6277)

... 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-6644-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6644.1
Version used: `2024-02-20T04:09:33Z`

References
`url: https://ubuntu.com/security/notices/USN-6644-1`
`cve: CVE-2023-52356`
`cve: CVE-2023-6228`
`cve: CVE-2023-6277`
`advisory_id: USN-6644-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-0219`
`cert-bund: WID-SEC-2023-3169`
`cert-bund: WID-SEC-2023-3004`
`dfn-cert: DFN-CERT-2024-1151`
`dfn-cert: DFN-CERT-2024-0649`
`dfn-cert: DFN-CERT-2024-0479`
`dfn-cert: DFN-CERT-2024-0446`
`dfn-cert: DFN-CERT-2024-0034`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5076-1)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5076-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   git
Installed version:    git-1:2.25.1-1ubuntu3.1
Fixed version:      >=git-1:2.25.1-1ubuntu3.2
```

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.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that Git allowed newline characters in certain repository paths. An attacker could potentially use this issue to perform cross-protocol requests.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5076-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5076.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5076-1`
`cve: CVE-2021-40330`
`advisory_id: USN-5076-1`
`cert-bund: WID-SEC-2022-1675`
`cert-bund: CB-K21/0963`
`dfn-cert: DFN-CERT-2022-2243`
`dfn-cert: DFN-CERT-2021-1914`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5080-1)

Summary
The remote host is missing an update for the 'libgcrypt20' package(s) announced via the USN-5080-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libgcrypt20
Installed version:    libgcrypt20-1.8.5-5ubuntu1
Fixed version:      >=libgcrypt20-1.8.5-5ubuntu1.1
```

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

Affected Software/OS
'libgcrypt20' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Libgcrypt incorrectly handled ElGamal encryption. An 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.

... continues on next page ...

... continued from previous page ...

Details: Ubuntu: Security Advisory (USN-5080-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5080.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5080-1
cve: CVE-2021-33560
cve: CVE-2021-40528
advisory_id: USN-5080-1
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0624
cert-bund: WID-SEC-2022-0623
cert-bund: WID-SEC-2022-0525
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1465
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-1947
dfn-cert: DFN-CERT-2021-1291

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3.8
Installed version: python3.8-3.8.5-1~20.04.3
Fixed version: >=python3.8-3.8.10-0ubuntu1~20.04.7

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

... continues on next page ...

... continued from previous page ...

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: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5960-1`
`cve: CVE-2023-24329`
`advisory_id: USN-5960-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2964`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-0513`
`dfn-cert: DFN-CERT-2023-2783`
`dfn-cert: DFN-CERT-2023-2542`
`dfn-cert: DFN-CERT-2023-2237`
`dfn-cert: DFN-CERT-2023-2227`
`dfn-cert: DFN-CERT-2023-1728`
`dfn-cert: DFN-CERT-2023-1667`
`dfn-cert: DFN-CERT-2023-1472`
`dfn-cert: DFN-CERT-2023-0571`
`dfn-cert: DFN-CERT-2023-0552`
`dfn-cert: DFN-CERT-2023-0527`
`dfn-cert: DFN-CERT-2023-0525`

High (CVSS: 7.5)
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:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.17
```

... continues on next page ...

... continued from previous page ...

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.
Details: `Ubuntu: Security Advisory (USN-6729-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6729.1
Version used: `2024-06-07T04:08:49Z`

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-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-0801`
`cert-bund: WID-SEC-2024-0789`
`dfn-cert: DFN-CERT-2024-1411`
`dfn-cert: DFN-CERT-2024-1335`
`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`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6506-1)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-6506-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   apache2
Installed version:    apache2-2.4.41-4ubuntu3.3
Fixed version:      >=apache2-2.4.41-4ubuntu3.15
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
David Shoon discovered that the Apache HTTP Server mod_macro module incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. (CVE-2023-31122)
Prof. Sven Dietrich, Isa Jafarov, Prof. Heejo Lee, and Choongin Lee discovered that the Apache HTTP Server incorrectly handled certain HTTP/2 connections. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. This issue only affected Ubuntu 23.04, and Ubuntu 23.10. (CVE-2023-43622)
Will Dormann and David Warren discovered that the Apache HTTP Server incorrectly handled memory when handling HTTP/2 connections. A remote attacker could possibly use this issue to cause the server to consume resources, leading to a denial of service. (CVE-2023-45802)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6506-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6506.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6506-1
cve: CVE-2023-31122
cve: CVE-2023-43622
cve: CVE-2023-45802
advisory_id: USN-6506-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0899
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0107
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2712
dfn-cert: DFN-CERT-2024-1411
dfn-cert: DFN-CERT-2024-1335
dfn-cert: DFN-CERT-2024-1152
dfn-cert: DFN-CERT-2024-1010
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0732
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-2640
dfn-cert: DFN-CERT-2023-2596
dfn-cert: DFN-CERT-2023-2583

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5342-1)

Summary
The remote host is missing an update for the 'python2.7, python3.4, python3.5, python3.6, python3.8' package(s) announced via the USN-5342-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   python3.8
Installed version:    python3.8-3.8.5-1~20.04.3
Fixed version:      >=python3.8-3.8.10-0ubuntu1~20.04.4
Vulnerable package:   python3.8-minimal
Installed version:    python3.8-minimal-3.8.5-1~20.04.3
Fixed version:      >=python3.8-minimal-3.8.10-0ubuntu1~20.04.4
```

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

Affected Software/OS
'python2.7, python3.4, python3.5, python3.6, python3.8' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
David Schworer discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-3426)

... continues on next page ...

... continued from previous page ...

It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. (CVE-2021-4189)
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. (CVE-2022-0391)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5342-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5342.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5342-1`
`cve: CVE-2021-3426`
`cve: CVE-2021-4189`
`cve: CVE-2022-0391`
`advisory_id: USN-5342-1`
`cert-bund: WID-SEC-2023-1418`
`cert-bund: WID-SEC-2023-0831`
`cert-bund: WID-SEC-2023-0426`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1308`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0624`
`cert-bund: WID-SEC-2022-0432`
`cert-bund: WID-SEC-2022-0302`
`cert-bund: WID-SEC-2022-0146`
`cert-bund: WID-SEC-2022-0011`
`cert-bund: CB-K22/0310`
`cert-bund: CB-K21/1268`
`dfn-cert: DFN-CERT-2023-2237`
`dfn-cert: DFN-CERT-2023-2227`
`dfn-cert: DFN-CERT-2023-1517`
`dfn-cert: DFN-CERT-2023-1472`
`dfn-cert: DFN-CERT-2023-1200`
`dfn-cert: DFN-CERT-2022-2020`
`dfn-cert: DFN-CERT-2022-1304`
`dfn-cert: DFN-CERT-2022-1294`
`dfn-cert: DFN-CERT-2022-1056`
`dfn-cert: DFN-CERT-2022-1053`
`dfn-cert: DFN-CERT-2022-0968`
`dfn-cert: DFN-CERT-2022-0865`
`dfn-cert: DFN-CERT-2022-0742`
`dfn-cert: DFN-CERT-2022-0690`
`dfn-cert: DFN-CERT-2022-0618`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0577
dfn-cert: DFN-CERT-2022-0576
dfn-cert: DFN-CERT-2022-0351
dfn-cert: DFN-CERT-2022-0223
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2354
dfn-cert: DFN-CERT-2021-2353
dfn-cert: DFN-CERT-2021-2207
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1407
dfn-cert: DFN-CERT-2021-0943
dfn-cert: DFN-CERT-2021-0682
dfn-cert: DFN-CERT-2021-0675
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6164-1)

Summary
The remote host is missing an update for the 'c-ares' package(s) announced via the USN-6164-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libc-ares2
Installed version:    libc-ares2-1.15.0-1build1
Fixed version:      >=libc-ares2-1.15.0-1ubuntu0.3
```

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

Affected Software/OS
'c-ares' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Hannes Moesl discovered that c-ares incorrectly handled certain ipv6 addresses. An attacker could use this issue to cause c-ares to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-31130)
Xiang Li discovered that c-ares incorrectly handled certain UDP packets. A remote attacker could possibly use this issue to cause c-res to crash, resulting in a denial of service. (CVE-2023-32067)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6164-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6164.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6164-1
cve: CVE-2023-31130
cve: CVE-2023-32067
advisory_id: USN-6164-1
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2057
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1475
cert-bund: WID-SEC-2023-1450
dfn-cert: DFN-CERT-2023-2987
dfn-cert: DFN-CERT-2023-2885
dfn-cert: DFN-CERT-2023-2772
dfn-cert: DFN-CERT-2023-1591
dfn-cert: DFN-CERT-2023-1483
dfn-cert: DFN-CERT-2023-1477
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1369
dfn-cert: DFN-CERT-2023-1316
dfn-cert: DFN-CERT-2023-1205

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5821-1)

Summary
The remote host is missing an update for the 'wheel' package(s) announced via the USN-5821-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3-wheel
Installed version: python3-wheel-0.34.2-1
Fixed version: >=python3-wheel-0.34.2-1ubuntu0.1

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
Sebastian Chnelik discovered that wheel incorrectly handled certain file names when validated against a regex expression. 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-5821-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5821.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5821-1`
`cve: CVE-2022-40898`
`advisory_id: USN-5821-1`
`cert-bund: WID-SEC-2023-2853`
`cert-bund: WID-SEC-2023-1424`
`dfn-cert: DFN-CERT-2023-2783`
`dfn-cert: DFN-CERT-2023-0718`
`dfn-cert: DFN-CERT-2023-0101`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5355-1)

Summary
The remote host is missing an update for the 'zlib' package(s) announced via the USN-5355-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   zlib1g
Installed version:    zlib1g-1:1.2.11.dfsg-2ubuntu1.2
Fixed version:      >=zlib1g-1:1.2.11.dfsg-2ubuntu1.3
```

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

Affected Software/OS
'zlib' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Danilo Ramos discovered that zlib incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause zlib to crash, resulting in 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-5355-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5355.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5355-1`
`cve: CVE-2018-25032`
`advisory_id: USN-5355-1`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1784`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-0141`
`cert-bund: WID-SEC-2023-0132`
`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-2022-0767`
`cert-bund: WID-SEC-2022-0736`
`cert-bund: WID-SEC-2022-0735`
`cert-bund: WID-SEC-2022-0677`
`cert-bund: WID-SEC-2022-0554`
`cert-bund: WID-SEC-2022-0005`
`cert-bund: CB-K22/0619`
`cert-bund: CB-K22/0386`
`dfn-cert: DFN-CERT-2024-0998`
`dfn-cert: DFN-CERT-2024-0790`
`dfn-cert: DFN-CERT-2023-3028`
`dfn-cert: DFN-CERT-2023-0553`
`dfn-cert: DFN-CERT-2023-0430`
`dfn-cert: DFN-CERT-2023-0121`
`dfn-cert: DFN-CERT-2023-0119`
`dfn-cert: DFN-CERT-2023-0100`
`dfn-cert: DFN-CERT-2022-2668`
`dfn-cert: DFN-CERT-2022-2305`

... continues on next page ...

... continued from previous page ...

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
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

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6078-1)

Summary
The remote host is missing an update for the 'libwebp' package(s) announced via the USN-6078-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libwebp6
Installed version:    libwebp6-0.6.1-2ubuntu0.20.04.1
Fixed version:      >=libwebp6-0.6.1-2ubuntu0.20.04.2
Vulnerable package:   libwebpdemux2
Installed version:    libwebpdemux2-0.6.1-2ubuntu0.20.04.1
Fixed version:      >=libwebpdemux2-0.6.1-2ubuntu0.20.04.2
Vulnerable package:   libwebpmux3
Installed version:    libwebpmux3-0.6.1-2ubuntu0.20.04.1
Fixed version:      >=libwebpmux3-0.6.1-2ubuntu0.20.04.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libwebp' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Irvan Kurniawan discovered that libwebp incorrectly handled certain memory operations. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in 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-6078-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6078.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6078-1`
`cve: CVE-2023-1999`
`advisory_id: USN-6078-1`
`cert-bund: WID-SEC-2023-2531`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1133`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-0998`
`dfn-cert: DFN-CERT-2023-0805`
`dfn-cert: DFN-CERT-2023-0804`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5625-1)

Summary
The remote host is missing an update for the 'mako' package(s) announced via the USN-5625-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-mako
Installed version:    python3-mako-1.1.0+ds1-1ubuntu2
Fixed version:      >=python3-mako-1.1.0+ds1-1ubuntu2.1
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
It was discovered that Mako incorrectly handled certain regular expressions. 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-5625-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5625.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5625-1`
`cve: CVE-2022-40023`
`advisory_id: USN-5625-1`
`cert-bund: WID-SEC-2023-2229`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-1185`
`dfn-cert: DFN-CERT-2022-2105`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5766-1)

Summary
The remote host is missing an update for the 'heimdal' package(s) announced via the USN-5766-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libwind0-heimdal
Installed version:    libwind0-heimdal-7.7.0+dfsg-1ubuntu1
Fixed version:      >=libwind0-heimdal-7.7.0+dfsg-1ubuntu1.2
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that Heimdal did not properly manage memory when normalizing Unicode. 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-5766-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5766.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5766-1`
`cve: CVE-2022-41916`
`advisory_id: USN-5766-1`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-2057`
`dfn-cert: DFN-CERT-2022-2777`
`dfn-cert: DFN-CERT-2022-2612`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6262-1)

Summary
The remote host is missing an update for the 'wireshark' package(s) announced via the USN-6262-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libwireshark13
Installed version:    libwireshark13-3.2.3-1
Fixed version:      >=libwireshark13-3.2.3-1ubuntu0.1~esm1
Vulnerable package:   wireshark
Installed version:    wireshark-3.2.3-1
Fixed version:      >=wireshark-3.2.3-1ubuntu0.1~esm1
Vulnerable package:   wireshark-common
Installed version:    wireshark-common-3.2.3-1
Fixed version:      >=wireshark-common-3.2.3-1ubuntu0.1~esm1
Vulnerable package:   wireshark-qt
Installed version:    wireshark-qt-3.2.3-1
Fixed version:      >=wireshark-qt-3.2.3-1ubuntu0.1~esm1
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
It was discovered that Wireshark did not properly handle certain NFS packages when certain configuration options were enabled. An attacker could possibly use this issue to cause Wireshark to crash, resulting in a denial of service. (CVE-2020-13164)
It was discovered that Wireshark did not properly handle certain GVCP packages. An attacker could possibly use this issue to cause Wireshark to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-15466)
It was discovered that Wireshark did not properly handle certain Kafka packages. An attacker could possibly use this issue to cause Wireshark to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-17498)
It was discovered that Wireshark did not properly handle certain TCP packages containing an invalid 0xFFFF checksum. An attacker could possibly use this issue to cause Wireshark to crash, resulting in a denial of service. (CVE-2020-25862)
It was discovered that Wireshark did not properly handle certain MIME packages containing invalid parts. An attacker could possibly use this issue to cause Wireshark to crash, resulting in a denial of service. (CVE-2020-25863)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6262-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6262.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6262-1`
`cve: CVE-2020-13164`
`cve: CVE-2020-15466`
`cve: CVE-2020-17498`
`cve: CVE-2020-25862`
`cve: CVE-2020-25863`
`advisory_id: USN-6262-1`
`cert-bund: WID-SEC-2023-1920`
`cert-bund: WID-SEC-2023-1919`
`cert-bund: WID-SEC-2023-1918`
`cert-bund: WID-SEC-2023-1917`
`cert-bund: CB-K20/0922`
`cert-bund: CB-K20/0820`
`cert-bund: CB-K20/0655`
`cert-bund: CB-K20/0485`
`dfn-cert: DFN-CERT-2023-1743`
`dfn-cert: DFN-CERT-2021-0257`
`dfn-cert: DFN-CERT-2020-2550`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-2078
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1796
dfn-cert: DFN-CERT-2020-1734
dfn-cert: DFN-CERT-2020-1448
dfn-cert: DFN-CERT-2020-1289
dfn-cert: DFN-CERT-2020-1075

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6303-1)

Summary
The remote host is missing an update for the 'clamav' package(s) announced via the USN-6303-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: clamav
Installed version: clamav-0.103.2+dfsg-0ubuntu0.20.04.2
Fixed version: >=clamav-0.103.9+dfsg-0ubuntu0.20.04.1

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

Affected Software/OS
'clamav' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that ClamAV incorrectly handled parsing HFS+ files. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6303-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6303.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6303-1
cve: CVE-2023-20197
advisory_id: USN-6303-1
cert-bund: WID-SEC-2023-2090
dfn-cert: DFN-CERT-2023-1936

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1905

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6168-1)

Summary
The remote host is missing an update for the 'libx11' package(s) announced via the USN-6168-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libx11-6
Installed version: libx11-6-2:1.6.9-2ubuntu1.2
Fixed version: >=libx11-6-2:1.6.9-2ubuntu1.5

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

Affected Software/OS
'libx11' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Gregory James Duck discovered that libx11 incorrectly handled certain Request, Event, or Error IDs. If a user were tricked into connecting to a malicious X Server, a remote attacker could possibly use this issue to cause libx11 to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6168-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6168.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6168-1
cve: CVE-2023-3138
advisory_id: USN-6168-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1485
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1391

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5996-1)

Summary
The remote host is missing an update for the 'liblouis' package(s) announced via the USN-5996-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   liblouis20
Installed version:    liblouis20-3.12.0-3
Fixed version:      >=liblouis20-3.12.0-3ubuntu0.2
```

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

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

Vulnerability Insight
It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-26767, CVE-2023-26768, CVE-2023-26769)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5996-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5996.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5996-1
cve: CVE-2023-26767
cve: CVE-2023-26768
cve: CVE-2023-26769
advisory_id: USN-5996-1
cert-bund: WID-SEC-2023-2853
cert-bund: WID-SEC-2023-2031
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-0859
dfn-cert: DFN-CERT-2023-0845
dfn-cert: DFN-CERT-2023-0762
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5233-1)

Summary
The remote host is missing an update for the 'clamav' package(s) announced via the USN-5233-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   clamav
Installed version:    clamav-0.103.2+dfsg-0ubuntu0.20.04.2
Fixed version:      >=clamav-0.103.5+dfsg-1~20.04.1
```

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

Affected Software/OS
'clamav' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that ClamAV incorrectly handled memory when the CL_SCAN_GENERAL_COLLECT_METADATA scan option was enabled. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5233-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5233.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5233-1
cve: CVE-2022-20698
advisory_id: USN-5233-1
cert-bund: WID-SEC-2022-0772
cert-bund: CB-K22/0052
dfn-cert: DFN-CERT-2022-0078
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5388-1)

Summary
The remote host is missing an update for the 'openjdk-lts' package(s) announced via the USN-5388-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.15+10-0ubuntu0.20.04.1
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.15+10-0ubuntu0.20.04.1
```

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

Affected Software/OS
'openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that OpenJDK incorrectly limited memory when compiling a specially crafted XPath expression. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21426)
It was discovered that OpenJDK incorrectly handled converting certain object arguments into their textual representations. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21434)
It was discovered that OpenJDK incorrectly validated the encoded length of certain object identifiers. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21443)
It was discovered that OpenJDK incorrectly validated certain paths. An attacker could possibly use this issue to bypass the secure validation feature and expose sensitive information in XML files. (CVE-2022-21476)
It was discovered that OpenJDK incorrectly parsed certain URI strings. An attacker could possibly use this issue to make applications accept invalid of malformed URI strings. (CVE-2022-21496)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5388-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5388.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5388-1
cve: CVE-2022-21426
cve: CVE-2022-21434
cve: CVE-2022-21443
cve: CVE-2022-21476
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-21496
advisory_id: USN-5388-1
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2022-1434
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1321
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1066
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0871
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0398
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0200
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0470
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2023-1174
dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0819
dfn-cert: DFN-CERT-2022-1955
dfn-cert: DFN-CERT-2022-1704
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1081
dfn-cert: DFN-CERT-2022-1054
dfn-cert: DFN-CERT-2022-0873
dfn-cert: DFN-CERT-2022-0871

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6142-1)

Summary
The remote host is missing an update for the 'nghttp2' package(s) announced via the USN-6142-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libnghttp2-14
Installed version:    libnghttp2-14-1.40.0-1build1
Fixed version:      >=libnghttp2-14-1.40.0-1ubuntu0.1
```

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.

Vulnerability Insight
Gal Goldshtein discovered that nghttp2 incorrectly handled certain inputs. 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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6142-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6142.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6142-1
cve: CVE-2020-11080
advisory_id: USN-6142-1
cert-bund: WID-SEC-2023-1374
cert-bund: CB-K20/1017
cert-bund: CB-K20/1015
cert-bund: CB-K20/0706
cert-bund: CB-K20/0544
dfn-cert: DFN-CERT-2023-2522
dfn-cert: DFN-CERT-2021-2172
dfn-cert: DFN-CERT-2021-0620
dfn-cert: DFN-CERT-2020-2139
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1962
dfn-cert: DFN-CERT-2020-1831
dfn-cert: DFN-CERT-2020-1615
dfn-cert: DFN-CERT-2020-1529
dfn-cert: DFN-CERT-2020-1501
dfn-cert: DFN-CERT-2020-1463
dfn-cert: DFN-CERT-2020-1335
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2020-1211
dfn-cert: DFN-CERT-2020-1164

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6505-1)

Summary
The remote host is missing an update for the 'nghttp2' package(s) announced via the USN-6505-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libnghttp2-14
Installed version: libnghttp2-14-1.40.0-1build1
Fixed version: >=libnghttp2-14-1.40.0-1ubuntu0.2

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

Affected Software/OS
'nghttp2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6505-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6505.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6505-1
cve: CVE-2023-44487
advisory_id: USN-6505-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1238
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0894
cert-bund: WID-SEC-2024-0887

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0874
cert-bund: WID-SEC-2024-0873
cert-bund: WID-SEC-2024-0870
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0794
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
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-2024-0830
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
dfn-cert: DFN-CERT-2024-0133
dfn-cert: DFN-CERT-2024-0129
dfn-cert: DFN-CERT-2024-0081

... continues on next page ...

... continued from previous page ...

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
dfn-cert: DFN-CERT-2023-2586
dfn-cert: DFN-CERT-2023-2585
dfn-cert: DFN-CERT-2023-2572

... continues on next page ...

... continued from previous page ...

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

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libnghttp2-14
Installed version: libnghttp2-14-1.40.0-1build1
Fixed version: >=libnghttp2-14-1.40.0-1ubuntu0.3

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.

... continues on next page ...

... continued from previous page ...

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-2024-1307`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1238`
`cert-bund: WID-SEC-2024-1228`
`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`
`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`

... continues on next page ...

... continued from previous page ...

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-2024-1367
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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

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

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5324-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-5324-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version:      >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.2
```

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could use this issue to cause libxml2 to crash, resulting in 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-5324-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5324.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5324-1
cve: CVE-2022-23308
advisory_id: USN-5324-1
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-1064
cert-bund: WID-SEC-2022-1057
cert-bund: WID-SEC-2022-0836
cert-bund: WID-SEC-2022-0774
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0735
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0339
cert-bund: CB-K22/0619
cert-bund: CB-K22/0617
cert-bund: CB-K22/0230
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1152
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1117
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1112
dfn-cert: DFN-CERT-2022-1105
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0787
dfn-cert: DFN-CERT-2022-0420

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5410-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5410-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libnss3
Installed version: libnss3-2:3.49.1-1ubuntu1.5
Fixed version: >=libnss3-2:3.49.1-1ubuntu1.7

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

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

Vulnerability Insight
Lenny Wang discovered that NSS incorrectly handled certain messages. A remote attacker could possibly use this issue to cause servers compiled with NSS to stop responding, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5410-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5410.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5410-1
cve: CVE-2020-25648
advisory_id: USN-5410-1

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K21/1095
cert-bund: CB-K21/0466
dfn-cert: DFN-CERT-2023-2661
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2196
dfn-cert: DFN-CERT-2021-2189
dfn-cert: DFN-CERT-2020-2362

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6832-1)

Summary
The remote host is missing an update for the 'virtuoso-opensource' package(s) announced via the USN-6832-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: virtuoso-opensource-6.1-bin
Installed version: virtuoso-opensource-6.1-bin-6.1.6+repack-0ubuntu10
Fixed version: >=virtuoso-opensource-6.1-bin-6.1.6+repack-0ubuntu10+esm1

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

Affected Software/OS
'virtuoso-opensource' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Jingzhou Fu discovered that Virtuoso Open-Source Edition incorrectly handled certain crafted SQL statements. An attacker could possibly use this issue to crash the program, resulting in a denial of service. (CVE-2023-31607, CVE-2023-31608, CVE-2023-31609, CVE-2023-31610, CVE-2023-31611, CVE-2023-31616, CVE-2023-31617, CVE-2023-31618, CVE-2023-31619, CVE-2023-31623, CVE-2023-31625, CVE-2023-31628)
Jingzhou Fu discovered that Virtuoso Open-Source Edition incorrectly handled certain crafted SQL statements. An attacker could possibly use this issue to crash the program, resulting in a denial of service. This issue only affects Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-31612, CVE-2023-31613, CVE-2023-31614, CVE-2023-31615)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6832-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2024.6832.1
Version used: 2024-06-14T04:07:51Z

References

```
url: https://ubuntu.com/security/notices/USN-6832-1
cve: CVE-2023-31607
cve: CVE-2023-31608
cve: CVE-2023-31609
cve: CVE-2023-31610
cve: CVE-2023-31611
cve: CVE-2023-31612
cve: CVE-2023-31613
cve: CVE-2023-31614
cve: CVE-2023-31615
cve: CVE-2023-31616
cve: CVE-2023-31617
cve: CVE-2023-31618
cve: CVE-2023-31619
cve: CVE-2023-31623
cve: CVE-2023-31625
cve: CVE-2023-31628
advisory_id: USN-6832-1
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6541-1)

Summary

The remote host is missing an update for the 'glibc' package(s) announced via the USN-6541-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libc-bin
Installed version:    libc-bin-2.31-0ubuntu9.2
Fixed version:      >=libc-bin-2.31-0ubuntu9.14
Vulnerable package:   libc6
Installed version:    libc6-2.31-0ubuntu9.2
Fixed version:      >=libc6-2.31-0ubuntu9.14
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'glibc' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that the GNU C Library was not properly handling certain memory operations. An attacker could possibly use this issue to cause a denial of service (application crash). (CVE-2023-4806, CVE-2023-4813)
It was discovered that the GNU C library was not properly implementing a fix for CVE-2023-4806 in certain cases, which could lead to a memory leak. An attacker could possibly use this issue to cause a denial of service (application crash). This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-5156)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6541-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6541.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6541-1`
`cve: CVE-2023-4806`
`cve: CVE-2023-4813`
`cve: CVE-2023-5156`
`advisory_id: USN-6541-1`
`cert-bund: WID-SEC-2023-2439`
`cert-bund: WID-SEC-2023-2384`
`cert-bund: WID-SEC-2023-2314`
`dfn-cert: DFN-CERT-2023-3068`
`dfn-cert: DFN-CERT-2023-2917`
`dfn-cert: DFN-CERT-2023-2481`
`dfn-cert: DFN-CERT-2023-2413`
`dfn-cert: DFN-CERT-2023-2372`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5422-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-5422-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version:      >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.3
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Shinji Sato discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 ESM, and Ubuntu 16.04 ESM. (CVE-2022-23308)
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-29824)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5422-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5422.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5422-1`
`cve: CVE-2022-23308`
`cve: CVE-2022-29824`
`advisory_id: USN-5422-1`
`cert-bund: WID-SEC-2023-2778`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2023-0132`
`cert-bund: WID-SEC-2022-1776`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-1438`
`cert-bund: WID-SEC-2022-1378`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-1064`
`cert-bund: WID-SEC-2022-1057`
`cert-bund: WID-SEC-2022-0836`
`cert-bund: WID-SEC-2022-0774`
`cert-bund: WID-SEC-2022-0767`
`cert-bund: WID-SEC-2022-0735`
`cert-bund: WID-SEC-2022-0602`
`cert-bund: WID-SEC-2022-0339`
`cert-bund: WID-SEC-2022-0008`

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0619
cert-bund: CB-K22/0617
cert-bund: CB-K22/0531
cert-bund: CB-K22/0230
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0969
dfn-cert: DFN-CERT-2023-0119
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2015
dfn-cert: DFN-CERT-2022-1669
dfn-cert: DFN-CERT-2022-1609
dfn-cert: DFN-CERT-2022-1605
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1599
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1183
dfn-cert: DFN-CERT-2022-1152
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-1117
dfn-cert: DFN-CERT-2022-1116
dfn-cert: DFN-CERT-2022-1115
dfn-cert: DFN-CERT-2022-1114
dfn-cert: DFN-CERT-2022-1112
dfn-cert: DFN-CERT-2022-1105
dfn-cert: DFN-CERT-2022-0981
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0787
dfn-cert: DFN-CERT-2022-0420

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5408-1)

Summary
The remote host is missing an update for the 'dnsmasq' package(s) announced via the USN-5408-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: dnsmasq-base
Installed version: dnsmasq-base-2.80-1.1ubuntu1.4
Fixed version: >=dnsmasq-base-2.80-1.1ubuntu1.5

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'dnsmasq' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Petr Mensik and Richard Johnson discovered that Dnsmasq incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or expose sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5408-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5408.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5408-1`
`cve: CVE-2022-0934`
`advisory_id: USN-5408-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-0137`
`cert-bund: WID-SEC-2022-1988`
`dfn-cert: DFN-CERT-2024-0829`
`dfn-cert: DFN-CERT-2022-0916`
`dfn-cert: DFN-CERT-2022-0906`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6034-1)

Summary
The remote host is missing an update for the 'dnsmasq' package(s) announced via the USN-6034-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   dnsmasq-base
Installed version:    dnsmasq-base-2.80-1.1ubuntu1.4
Fixed version:      >=dnsmasq-base-2.80-1.1ubuntu1.7
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'dnsmasq' 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 Dnsmasq was sending large DNS messages over UDP, possibly causing transmission failures due to IP fragmentation. This update lowers the default maximum size of DNS messages to improve transmission reliability over UDP.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6034-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6034.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6034-1`
`cve: CVE-2023-28450`
`advisory_id: USN-6034-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-0668`
`dfn-cert: DFN-CERT-2024-0829`
`dfn-cert: DFN-CERT-2024-0498`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-0927`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-6657-1)

Summary
The remote host is missing an update for the 'dnsmasq' package(s) announced via the USN-6657-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   dnsmasq-base
Installed version:    dnsmasq-base-2.80-1.1ubuntu1.4
Fixed version:      >=dnsmasq-base-2.90-0ubuntu0.20.04.1
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
Elias Heftrig, Haya Schulmann, Niklas Vogel, and Michael Waidner discovered that Dnsmasq icorrectly handled validating DNSSEC messages. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. (CVE-2023-50387)
It was discovered that Dnsmasq incorrectly handled preparing an NSEC3 closest encloser proof. A remote attacker could possibly use this issue to cause Dnsmasq to consume resources, leading to a denial of service. (CVE-2023-50868)
It was discovered that Dnsmasq incorrectly set the maximum EDNS.0 UDP packet size as required by DNS Flag Day 2020. This issue only affected Ubuntu 23.10. (CVE-2023-28450)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6657-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6657.1
Version used: `2024-02-27T04:09:22Z`

References
`url: https://ubuntu.com/security/notices/USN-6657-1`
`cve: CVE-2023-28450`
`cve: CVE-2023-50387`
`cve: CVE-2023-50868`
`advisory_id: USN-6657-1`
`cert-bund: WID-SEC-2024-1347`
`cert-bund: WID-SEC-2024-1313`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0387`
`cert-bund: WID-SEC-2024-0386`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-0668`
`dfn-cert: DFN-CERT-2024-1523`
`dfn-cert: DFN-CERT-2024-1516`
`dfn-cert: DFN-CERT-2024-1474`
`dfn-cert: DFN-CERT-2024-1413`
`dfn-cert: DFN-CERT-2024-1223`
`dfn-cert: DFN-CERT-2024-1011`
`dfn-cert: DFN-CERT-2024-0984`
`dfn-cert: DFN-CERT-2024-0977`
`dfn-cert: DFN-CERT-2024-0921`
`dfn-cert: DFN-CERT-2024-0829`
`dfn-cert: DFN-CERT-2024-0529`
`dfn-cert: DFN-CERT-2024-0498`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0404
dfn-cert: DFN-CERT-2024-0399
dfn-cert: DFN-CERT-2024-0387
dfn-cert: DFN-CERT-2024-0379
dfn-cert: DFN-CERT-2024-0375
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-0927

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5526-1)

Summary
The remote host is missing an update for the 'pyjwt' package(s) announced via the USN-5526-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3-jwt
Installed version: python3-jwt-1.7.1-2ubuntu2
Fixed version: >=python3-jwt-1.7.1-2ubuntu2.1

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

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

Vulnerability Insight
Aapo Oksman discovered that PyJWT incorrectly handled signatures constructed from SSH public keys. A remote attacker could use this to forge a JWT signature.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5526-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5526.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5526-1
cve: CVE-2022-29217
advisory_id: USN-5526-1
cert-bund: WID-SEC-2022-1893
cert-bund: WID-SEC-2022-0456

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1177

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5425-1)

Summary
The remote host is missing an update for the 'pcre3' package(s) announced via the USN-5425-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpcre3
Installed version: libpcre3-2:8.39-12build1
Fixed version: >=libpcre3-2:8.39-12ubuntu0.1

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

Affected Software/OS
'pcre3' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Yunho Kim discovered that PCRE incorrectly handled memory when handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to expose sensitive information. This issue only affects Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 21.10 and Ubuntu 22.04 LTS. (CVE-2019-20838)
It was discovered that PCRE incorrectly handled memory when handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to have unexpected behavior. This issue only affects Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-14155)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5425-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5425.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5425-1
cve: CVE-2019-20838
cve: CVE-2020-14155
advisory_id: USN-5425-1

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1897
cert-bund: WID-SEC-2022-1772
cert-bund: CB-K21/0112
cert-bund: CB-K20/1120
dfn-cert: DFN-CERT-2024-0790
dfn-cert: DFN-CERT-2023-3028
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2380
dfn-cert: DFN-CERT-2021-2245
dfn-cert: DFN-CERT-2021-0216
dfn-cert: DFN-CERT-2020-2499
dfn-cert: DFN-CERT-2020-1424

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: rsync
Installed version: rsync-3.1.3-8
Fixed version: >=rsync-3.1.3-8ubuntu0.5

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

... continues on next page ...

... continued from previous page ...

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: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5921-1
cve: CVE-2022-29154
advisory_id: USN-5921-1
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0831
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0891
dfn-cert: DFN-CERT-2023-1162
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
dfn-cert: DFN-CERT-2022-1835
dfn-cert: DFN-CERT-2022-1710

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-6077-1)

Summary
The remote host is missing an update for the 'openjdk-8, openjdk-17, openjdk-20, openjdk-lts' package(s) announced via the USN-6077-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: openjdk-11-jre
Installed version: openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-11.0.19+7~us1-0ubuntu1~20.04.1
Vulnerable package: openjdk-11-jre-headless
Installed version: openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-headless-11.0.19+7~us1-0ubuntu1~20.04.1
Vulnerable package: openjdk-8-jdk
Installed version: openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version: >=openjdk-8-jdk-8u372-ga~us1-0ubuntu1~20.04
Vulnerable package: openjdk-8-jre
Installed version: openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version: >=openjdk-8-jre-8u372-ga~us1-0ubuntu1~20.04

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u372-ga~us1-0ubuntu1~20.04
```

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

Affected Software/OS
'openjdk-8, openjdk-17, openjdk-20, openjdk-lts' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Ben Smyth discovered that OpenJDK incorrectly handled half-duplex connections during TLS handshake. A remote attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-21930)
It was discovered that OpenJDK incorrectly handled certain inputs. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-21937)
It was discovered that OpenJDK incorrectly handled command arguments. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-21938)
It was discovered that OpenJDK incorrectly validated HTML documents. An attacker could possibly use this issue to insert, edit or obtain sensitive information. (CVE-2023-21939)
Ramki Ramakrishna discovered that OpenJDK incorrectly handled garbage collection. An attacker could possibly use this issue to bypass Java sandbox restrictions. (CVE-2023-21954)
Jonathan Looney discovered that OpenJDK incorrectly handled certificate chains during TLS session negotiation. A remote attacker could possibly use this issue to cause a denial of service. (CVE-2023-21967)
Adam Reziouk discovered that OpenJDK incorrectly sanitized URIs. An attacker could possibly use this issue to bypass Java sandbox restrictions. (CVE-2023-21968)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6077-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6077.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6077-1
cve: CVE-2023-21930
cve: CVE-2023-21937
cve: CVE-2023-21938
cve: CVE-2023-21939
cve: CVE-2023-21954
cve: CVE-2023-21967
cve: CVE-2023-21968
advisory_id: USN-6077-1
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2112
cert-bund: WID-SEC-2023-1846
cert-bund: WID-SEC-2023-1011
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2493
dfn-cert: DFN-CERT-2023-2249
dfn-cert: DFN-CERT-2023-2240
dfn-cert: DFN-CERT-2023-1955
dfn-cert: DFN-CERT-2023-1909
dfn-cert: DFN-CERT-2023-1879
dfn-cert: DFN-CERT-2023-1605
dfn-cert: DFN-CERT-2023-1418
dfn-cert: DFN-CERT-2023-1336
dfn-cert: DFN-CERT-2023-1304
dfn-cert: DFN-CERT-2023-0897
dfn-cert: DFN-CERT-2023-0896

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-6660-1)

Summary
The remote host is missing an update for the 'openjdk-lts' package(s) announced via the USN-6660-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.22+7-0ubuntu2~20.04.1
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.22+7-0ubuntu2~20.04.1
```

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

Affected Software/OS
'openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Yi Yang discovered that the Hotspot component of OpenJDK 11 incorrectly handled array accesses in the C1 compiler. An attacker could possibly use this issue to cause a denial of service, execute arbitrary code or bypass Java sandbox restrictions. (CVE-2024-20918)
It was discovered that the Hotspot component of OpenJDK 11 did not properly verify bytecode in certain situations. An attacker could possibly use this issue to bypass Java sandbox restrictions. (CVE-2024-20919)
It was discovered that the Hotspot component of OpenJDK 11 had an optimization flaw when generating range check loop predicates. An attacker could possibly use this issue to cause a denial of service, execute arbitrary code or bypass Java sandbox restrictions. (CVE-2024-20921)
Valentin Eudeline discovered that OpenJDK 11 incorrectly handled certain options in the Nashorn JavaScript subcomponent. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-20926)
It was discovered that OpenJDK 11 could produce debug logs that contained private keys used for digital signatures. An attacker could possibly use this issue to obtain sensitive information. (CVE-2024-20945)
Hubert Kario discovered that the TLS implementation in OpenJDK 11 had a timing side-channel and incorrectly handled RSA padding. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2024-20952)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6660-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6660.1
Version used: `2024-02-27T04:09:22Z`

References
`url: https://ubuntu.com/security/notices/USN-6660-1`
`cve: CVE-2024-20918`
`cve: CVE-2024-20919`
`cve: CVE-2024-20921`
`cve: CVE-2024-20926`
`cve: CVE-2024-20945`
`cve: CVE-2024-20952`
`advisory_id: USN-6660-1`
`cert-bund: WID-SEC-2024-0769`
`cert-bund: WID-SEC-2024-0121`
`dfn-cert: DFN-CERT-2024-0533`
`dfn-cert: DFN-CERT-2024-0502`
`dfn-cert: DFN-CERT-2024-0501`
`dfn-cert: DFN-CERT-2024-0500`
`dfn-cert: DFN-CERT-2024-0494`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2024-0422`
`dfn-cert: DFN-CERT-2024-0417`
`dfn-cert: DFN-CERT-2024-0361`
`dfn-cert: DFN-CERT-2024-0354`
`dfn-cert: DFN-CERT-2024-0129`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0128

High (CVSS: 7.4)
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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgnutls30
Installed version: libgnutls30-3.6.13-2ubuntu1.3
Fixed version: >=libgnutls30-3.6.13-2ubuntu1.8

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: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5901-1
cve: CVE-2023-0361
advisory_id: USN-5901-1
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0353
dfn-cert: DFN-CERT-2024-0940
dfn-cert: DFN-CERT-2023-3203

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1939
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1448
dfn-cert: DFN-CERT-2023-1285
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0374

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-6696-1)

Summary
The remote host is missing an update for the 'openjdk-8' package(s) announced via the USN-6696-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u402-ga-2ubuntu1~20.04
Vulnerable package:   openjdk-8-jdk-headless
Installed version:    openjdk-8-jdk-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-headless-8u402-ga-2ubuntu1~20.04
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u402-ga-2ubuntu1~20.04
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u402-ga-2ubuntu1~20.04
```

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

Affected Software/OS
'openjdk-8' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
Yi Yang discovered that the Hotspot component of OpenJDK 8 incorrectly handled array accesses in the C1 compiler. An attacker could possibly use this issue to cause a denial of service, execute arbitrary code or bypass Java sandbox restrictions. (CVE-2024-20918)
It was discovered that the Hotspot component of OpenJDK 8 did not properly verify bytecode in certain situations. An attacker could possibly use this issue to bypass Java sandbox restrictions. (CVE-2024-20919)

... continues on next page ...

... continued from previous page ...

It was discovered that the Hotspot component of OpenJDK 8 had an optimization flaw when generating range check loop predicates. An attacker could possibly use this issue to cause a denial of service, execute arbitrary code or bypass Java sandbox restrictions. (CVE-2024-20921)
Valentin Eudeline discovered that OpenJDK 8 incorrectly handled certain options in the Nashorn JavaScript subcomponent. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-20926)
It was discovered that OpenJDK 8 could produce debug logs that contained private keys used for digital signatures. An attacker could possibly use this issue to obtain sensitive information. (CVE-2024-20945)
Hubert Kario discovered that the TLS implementation in OpenJDK 8 had a timing side-channel and incorrectly handled RSA padding. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2024-20952)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6696-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6696.1
Version used: `2024-03-18T08:50:22Z`

References
`url: https://ubuntu.com/security/notices/USN-6696-1`
`cve: CVE-2024-20918`
`cve: CVE-2024-20919`
`cve: CVE-2024-20921`
`cve: CVE-2024-20926`
`cve: CVE-2024-20945`
`cve: CVE-2024-20952`
`advisory_id: USN-6696-1`
`cert-bund: WID-SEC-2024-0769`
`cert-bund: WID-SEC-2024-0121`
`dfn-cert: DFN-CERT-2024-0533`
`dfn-cert: DFN-CERT-2024-0502`
`dfn-cert: DFN-CERT-2024-0501`
`dfn-cert: DFN-CERT-2024-0500`
`dfn-cert: DFN-CERT-2024-0494`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2024-0422`
`dfn-cert: DFN-CERT-2024-0417`
`dfn-cert: DFN-CERT-2024-0361`
`dfn-cert: DFN-CERT-2024-0354`
`dfn-cert: DFN-CERT-2024-0129`
`dfn-cert: DFN-CERT-2024-0128`

High (CVSS: 7.3)
NVT: Ubuntu: Security Advisory (USN-6666-1)

... continues on next page ...

. . . continued from previous page . . .

Summary
The remote host is missing an update for the 'libuv1' package(s) announced via the USN-6666-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libuv1
Installed version:    libuv1-1.34.2-1ubuntu1.1
Fixed version:      >=libuv1-1.34.2-1ubuntu1.5
```

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

Affected Software/OS
'libuv1' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that libuv incorrectly truncated certain hostnames. A remote attacker could possibly use this issue with specially crafted hostnames to bypass certain checks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6666-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6666.1
Version used: `2024-02-29T04:08:50Z`

References
```
url: https://ubuntu.com/security/notices/USN-6666-1
cve: CVE-2024-24806
advisory_id: USN-6666-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-0540
cert-bund: WID-SEC-2024-0393
dfn-cert: DFN-CERT-2024-1274
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0994
dfn-cert: DFN-CERT-2024-0536
dfn-cert: DFN-CERT-2024-0531
```

High (CVSS: 7.3)
NVT: Ubuntu: Security Advisory (USN-6566-1)

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'sqlite3' package(s) announced via the USN-6566-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libsqlite3-0
Installed version:    libsqlite3-0-3.31.1-4ubuntu0.2
Fixed version:      >=libsqlite3-0-3.31.1-4ubuntu0.6
```

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

Affected Software/OS
'sqlite3' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that SQLite incorrectly handled certain protection mechanisms when using a CLI script with the –safe option, contrary to expectations. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-46908)
It was discovered that SQLite incorrectly handled certain memory operations in the sessions extension. A remote attacker could possibly use this issue to cause SQLite to crash, resulting in a denial of service. (CVE-2023-7104)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6566-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6566.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6566-1
cve: CVE-2022-46908
cve: CVE-2023-7104
advisory_id: USN-6566-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0521
cert-bund: WID-SEC-2024-0119
cert-bund: WID-SEC-2024-0092
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1022
cert-bund: WID-SEC-2023-1017
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1016
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1102
dfn-cert: DFN-CERT-2024-0791
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0127
dfn-cert: DFN-CERT-2024-0115
dfn-cert: DFN-CERT-2024-0030
dfn-cert: DFN-CERT-2024-0020
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2022-2904

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-6184-1)

Summary
The remote host is missing an update for the 'cups' package(s) announced via the USN-6184-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: cups
Installed version: cups-2.3.1-9ubuntu1.1
Fixed version: >=cups-2.3.1-9ubuntu1.4

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

Affected Software/OS
'cups' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that CUPS incorrectly handled certain memory operations. An attacker could possibly use this issue to cause CUPS to crash, resulting in a denial of service, or possibly obtain sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6184-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6184.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-6184-1
cve: CVE-2023-34241
advisory_id: USN-6184-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1540
dfn-cert: DFN-CERT-2023-2770
dfn-cert: DFN-CERT-2023-2229
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1700
dfn-cert: DFN-CERT-2023-1698
dfn-cert: DFN-CERT-2023-1691
dfn-cert: DFN-CERT-2023-1455

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5267-1)

Summary

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5267-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.97.101

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

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

It was discovered that the Bluetooth subsystem 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-2021-3640)

... continues on next page ...

... continued from previous page ...

Likang Luo discovered that a race condition existed in the Bluetooth subsystem of 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-2021-3752)
Luo Likang discovered that the FireDTV Firewire driver in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-42739)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5267-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5267.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5267-1`
`cve: CVE-2021-3640`
`cve: CVE-2021-3752`
`cve: CVE-2021-42739`
`advisory_id: USN-5267-1`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-1992`
`cert-bund: WID-SEC-2022-0676`
`cert-bund: WID-SEC-2022-0225`
`cert-bund: WID-SEC-2022-0223`
`cert-bund: CB-K21/1086`
`cert-bund: CB-K21/0978`
`cert-bund: CB-K21/0801`
`dfn-cert: DFN-CERT-2024-0333`
`dfn-cert: DFN-CERT-2023-0606`
`dfn-cert: DFN-CERT-2023-0127`
`dfn-cert: DFN-CERT-2022-2569`
`dfn-cert: DFN-CERT-2022-2510`
`dfn-cert: DFN-CERT-2022-2502`
`dfn-cert: DFN-CERT-2022-2448`
`dfn-cert: DFN-CERT-2022-2268`
`dfn-cert: DFN-CERT-2022-1575`
`dfn-cert: DFN-CERT-2022-1571`
`dfn-cert: DFN-CERT-2022-1519`
`dfn-cert: DFN-CERT-2022-1294`
`dfn-cert: DFN-CERT-2022-1057`
`dfn-cert: DFN-CERT-2022-0737`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0548`
`dfn-cert: DFN-CERT-2022-0547`
`dfn-cert: DFN-CERT-2022-0436`
`dfn-cert: DFN-CERT-2022-0354`
`dfn-cert: DFN-CERT-2022-0262`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0261
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0258
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0237
dfn-cert: DFN-CERT-2022-0194
dfn-cert: DFN-CERT-2022-0058
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2440
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2343
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2137
dfn-cert: DFN-CERT-2021-2135
dfn-cert: DFN-CERT-2021-2134
dfn-cert: DFN-CERT-2021-2133
dfn-cert: DFN-CERT-2021-2132
dfn-cert: DFN-CERT-2021-2120
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1938

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5421-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5421-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version:      >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.3
```

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 21.10.

Vulnerability Insight
It was discovered that LibTIFF incorrectly handled certain images. An attacker could possibly use this issue to cause a crash, resulting in a denial of service. This issue only affects Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-35522)
Chintan Shah discovered that LibTIFF incorrectly handled memory when handling certain images. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-0561, CVE-2022-0562, CVE-2022-0891)
It was discovered that LibTIFF incorrectly handled certain images. An attacker could possibly use this issue to cause a crash, resulting in a denial of service. This issue only affects Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2022-0865)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5421-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5421.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5421-1
cve: CVE-2020-35522
cve: CVE-2022-0561
cve: CVE-2022-0562
cve: CVE-2022-0865
cve: CVE-2022-0891
advisory_id: USN-5421-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0922
cert-bund: WID-SEC-2022-0914
cert-bund: WID-SEC-2022-0150
dfn-cert: DFN-CERT-2022-2592
dfn-cert: DFN-CERT-2022-2494
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2351
dfn-cert: DFN-CERT-2022-1109
dfn-cert: DFN-CERT-2022-1106
dfn-cert: DFN-CERT-2022-0682
dfn-cert: DFN-CERT-2022-0641
dfn-cert: DFN-CERT-2022-0504
dfn-cert: DFN-CERT-2022-0395
dfn-cert: DFN-CERT-2022-0389
dfn-cert: DFN-CERT-2022-0363
dfn-cert: DFN-CERT-2021-2371
dfn-cert: DFN-CERT-2021-0702

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5030-1)

Summary
The remote host is missing an update for the 'libdbi-perl' package(s) announced via the USN-5030-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libdbi-perl
Installed version: libdbi-perl-1.643-1
Fixed version: >=libdbi-perl-1.643-1ubuntu0.1

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

Affected Software/OS
'libdbi-perl' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the Perl DBI module incorrectly opened files outside of the folder specified in the data source name. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2014-10402)
It was discovered that the Perl DBI module incorrectly handled certain long strings. A local attacker could possibly use this issue to cause the DBI module to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2020-14393)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5030-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5030.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5030-1
cve: CVE-2014-10402
cve: CVE-2020-14393
advisory_id: USN-5030-1
cert-bund: WID-SEC-2024-1248
cert-bund: CB-K20/1149
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2021-1657
dfn-cert: DFN-CERT-2020-2554
dfn-cert: DFN-CERT-2020-2011

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5643-1)

Summary

The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-5643-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: ghostscript
Installed version: ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version: >=ghostscript-9.50~dfsg-5ubuntu4.6

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

Affected Software/OS

'ghostscript' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight

It was discovered that GhostScript incorrectly handled certain PDF files. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to cause GhostScript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-27792)
It was discovered that GhostScript incorrectly handled certain PDF files. If a user or automated system were tricked into opening a specially crafted PDF file, a remote attacker could use this issue to cause GhostScript to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-2085)

... 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-5643-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5643.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5643-1`
`cve: CVE-2020-27792`
`cve: CVE-2022-2085`
`advisory_id: USN-5643-1`
`cert-bund: WID-SEC-2022-1490`
`cert-bund: WID-SEC-2022-0383`
`dfn-cert: DFN-CERT-2022-2141`
`dfn-cert: DFN-CERT-2022-1944`
`dfn-cert: DFN-CERT-2022-1693`

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5267-2)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-5267-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.99.103
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

USN-5267-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused the kernel to freeze when accessing CIFS shares in some situations. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that the Bluetooth subsystem 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-2021-3640)
Likang Luo discovered that a race condition existed in the Bluetooth subsystem of 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-2021-3752)
Luo Likang discovered that the FireDTV Firewire driver in the Linux kernel did not properly perform bounds checking in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-42739)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5267-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5267.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5267-2`
`url: https://launchpad.net/bugs/1959665`
`cve: CVE-2021-3640`
`cve: CVE-2021-3752`
`cve: CVE-2021-42739`
`advisory_id: USN-5267-2`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2022-1992`
`cert-bund: WID-SEC-2022-0676`
`cert-bund: WID-SEC-2022-0225`
`cert-bund: WID-SEC-2022-0223`
`cert-bund: CB-K21/1086`
`cert-bund: CB-K21/0978`
`cert-bund: CB-K21/0801`
`dfn-cert: DFN-CERT-2024-0333`
`dfn-cert: DFN-CERT-2023-0606`
`dfn-cert: DFN-CERT-2023-0127`
`dfn-cert: DFN-CERT-2022-2569`
`dfn-cert: DFN-CERT-2022-2510`
`dfn-cert: DFN-CERT-2022-2502`
`dfn-cert: DFN-CERT-2022-2448`
`dfn-cert: DFN-CERT-2022-2268`
`dfn-cert: DFN-CERT-2022-1575`
`dfn-cert: DFN-CERT-2022-1571`
`dfn-cert: DFN-CERT-2022-1519`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0737
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0436
dfn-cert: DFN-CERT-2022-0354
dfn-cert: DFN-CERT-2022-0262
dfn-cert: DFN-CERT-2022-0261
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0258
dfn-cert: DFN-CERT-2022-0240
dfn-cert: DFN-CERT-2022-0237
dfn-cert: DFN-CERT-2022-0194
dfn-cert: DFN-CERT-2022-0058
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2021-2637
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2513
dfn-cert: DFN-CERT-2021-2493
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2440
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2343
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2137
dfn-cert: DFN-CERT-2021-2135
dfn-cert: DFN-CERT-2021-2134
dfn-cert: DFN-CERT-2021-2133
dfn-cert: DFN-CERT-2021-2132
dfn-cert: DFN-CERT-2021-2120
dfn-cert: DFN-CERT-2021-2007
dfn-cert: DFN-CERT-2021-2006
dfn-cert: DFN-CERT-2021-1991
dfn-cert: DFN-CERT-2021-1978
dfn-cert: DFN-CERT-2021-1977
dfn-cert: DFN-CERT-2021-1938

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-6373-1)

Summary
The remote host is missing an update for the 'gawk' package(s) announced via the USN-6373-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   gawk
Installed version:    gawk-1:5.0.1+dfsg-1
Fixed version:      >=gawk-1:5.0.1+dfsg-1ubuntu0.1
```

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

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

Vulnerability Insight
It was discovered that gawk could be made to read out of bounds when processing certain inputs. If a user or an automated system were tricked into opening a specially crafted input, 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-6373-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6373.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6373-1
cve: CVE-2023-4156
advisory_id: USN-6373-1
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-1976
```

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-6625-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6625-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.171.169
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Marek Marczykowski-Gorecki discovered that the Xen event channel infrastructure implementation in the Linux kernel contained a race condition. An attacker in a guest VM could possibly use this to cause a denial of service (paravirtualized device unavailability). (CVE-2023-34324)
Zheng Wang discovered a use-after-free in the Renesas Ethernet AVB driver in the Linux kernel during device removal. A privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-35827)
It was discovered that a race condition existed in the Linux kernel when performing operations with kernel objects, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2023-45863)
Huang Si Cong discovered that the NFC Controller Interface (NCI) implementation in the Linux kernel did not properly handle certain memory allocation failure conditions, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-46343)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6625-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6625.1
Version used: `2024-02-08T04:08:50Z`

References

```
url: https://ubuntu.com/security/notices/USN-6625-1
cve: CVE-2023-34324
cve: CVE-2023-35827
```

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-45863
cve: CVE-2023-46343
advisory_id: USN-6625-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0182
cert-bund: WID-SEC-2023-2643
cert-bund: WID-SEC-2023-2617
cert-bund: WID-SEC-2023-1503
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1398
dfn-cert: DFN-CERT-2024-1381
dfn-cert: DFN-CERT-2024-1309
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1165
dfn-cert: DFN-CERT-2024-1122
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-2024-0863
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-2024-0750
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0630
dfn-cert: DFN-CERT-2024-0611
dfn-cert: DFN-CERT-2024-0487
dfn-cert: DFN-CERT-2024-0406
dfn-cert: DFN-CERT-2024-0371
dfn-cert: DFN-CERT-2024-0370
dfn-cert: DFN-CERT-2024-0351
dfn-cert: DFN-CERT-2024-0326
dfn-cert: DFN-CERT-2024-0325
dfn-cert: DFN-CERT-2024-0320
dfn-cert: DFN-CERT-2024-0237
dfn-cert: DFN-CERT-2024-0235
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0095
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2024-0082
dfn-cert: DFN-CERT-2024-0015
dfn-cert: DFN-CERT-2023-3123
dfn-cert: DFN-CERT-2023-3121

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-3120
dfn-cert: DFN-CERT-2023-3114
dfn-cert: DFN-CERT-2023-3113
dfn-cert: DFN-CERT-2023-2800
dfn-cert: DFN-CERT-2023-2745
dfn-cert: DFN-CERT-2023-2744
dfn-cert: DFN-CERT-2023-2743
dfn-cert: DFN-CERT-2023-2725
dfn-cert: DFN-CERT-2023-2723
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2721
dfn-cert: DFN-CERT-2023-2720
dfn-cert: DFN-CERT-2023-2719
dfn-cert: DFN-CERT-2023-2718
dfn-cert: DFN-CERT-2023-2683
dfn-cert: DFN-CERT-2023-2442
dfn-cert: DFN-CERT-2023-2441

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-6565-1)

Summary
The remote host is missing an update for the 'openssh' package(s) announced via the USN-6565-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: openssh-client
Installed version: openssh-client-1:8.2p1-4ubuntu0.2
Fixed version: >=openssh-client-1:8.2p1-4ubuntu0.11
Vulnerable package: openssh-server
Installed version: openssh-server-1:8.2p1-4ubuntu0.2
Fixed version: >=openssh-server-1:8.2p1-4ubuntu0.11

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

Affected Software/OS
'openssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that OpenSSH incorrectly handled supplemental groups when running helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand as a different user. An attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 20.04 LTS. (CVE-2021-41617)
It was discovered that OpenSSH incorrectly added destination constraints when PKCS#11 token keys were added to ssh-agent, contrary to expectations. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-51384)
It was discovered that OpenSSH incorrectly handled user names or host names with shell metacharacters. An attacker could possibly use this issue to perform OS command injection. (CVE-2023-51385)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6565-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6565.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6565-1`
`cve: CVE-2021-41617`
`cve: CVE-2023-51384`
`cve: CVE-2023-51385`
`advisory_id: USN-6565-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1082`
`cert-bund: WID-SEC-2024-0578`
`cert-bund: WID-SEC-2023-3182`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-0426`
`cert-bund: WID-SEC-2022-1308`
`cert-bund: WID-SEC-2022-0676`
`cert-bund: WID-SEC-2022-0534`
`cert-bund: CB-K22/0310`
`cert-bund: CB-K22/0011`
`cert-bund: CB-K21/1268`
`cert-bund: CB-K21/1017`
`dfn-cert: DFN-CERT-2024-1260`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0744`
`dfn-cert: DFN-CERT-2024-0633`
`dfn-cert: DFN-CERT-2024-0545`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2024-0480`
`dfn-cert: DFN-CERT-2024-0092`
`dfn-cert: DFN-CERT-2024-0088`
`dfn-cert: DFN-CERT-2024-0022`
`dfn-cert: DFN-CERT-2023-3218`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3175
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-0579
dfn-cert: DFN-CERT-2021-2586
dfn-cert: DFN-CERT-2021-2017
dfn-cert: DFN-CERT-2021-2015

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-5753-1)

Summary
The remote host is missing an update for the 'snapd' package(s) announced via the USN-5753-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: snapd
Installed version: snapd-2.49.2+20.04
Fixed version: >=snapd-2.57.5+20.04ubuntu0.1

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

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

Vulnerability Insight
The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing the private /tmp mount for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5753-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5753.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5753-1
cve: CVE-2022-3328
advisory_id: USN-5753-1
cert-bund: WID-SEC-2022-2224

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2723

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-6391-1)

Summary
The remote host is missing an update for the 'cups' package(s) announced via the USN-6391-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: cups
Installed version: cups-2.3.1-9ubuntu1.1
Fixed version: >=cups-2.3.1-9ubuntu1.6

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

Affected Software/OS
'cups' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that CUPS incorrectly parsed certain Postscript objects. If a user or automated system were tricked into printing a specially crafted document, a remote attacker could use this issue to cause CUPS to crash, resulting in 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-6391-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6391.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6391-1
cve: CVE-2023-4504
advisory_id: USN-6391-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2402
dfn-cert: DFN-CERT-2023-2542
dfn-cert: DFN-CERT-2023-2231
dfn-cert: DFN-CERT-2023-2229
dfn-cert: DFN-CERT-2023-2225

[return to 192.168.218.129]

2.1.2 High general/tcp

High (CVSS: 7.5)
NVT: Wireshark Security Update (wnpa-sec-2020-09) - Linux

Product detection result
cpe:/a:wireshark:wireshark:3.2.3
Detected by Wireshark Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1
↪.0.800039)

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

Quality of Detection: 80

Vulnerability Detection Result
Installed version: 3.2.3
Fixed version: 3.2.5
Installation
path / port: /usr/bin/wireshark

Impact
Successful exploitation may allow remote attackers perform denial of service.

Solution:
Solution type: VendorFix
Update to version 3.2.5 or later.

Affected Software/OS
Wireshark versions 3.2.0 to 3.2.4.

Vulnerability Insight
The flaw exists due to GVCP dissector could go into an infinite loop.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Wireshark Security Update (wnpa-sec-2020-09) - Linux
OID:1.3.6.1.4.1.25623.1.0.817216
Version used: 2021-10-04T14:22:38Z

Product Detection Result
Product: cpe:/a:wireshark:wireshark:3.2.3
Method: Wireshark Detection (Linux/Unix SSH Login)
OID: 1.3.6.1.4.1.25623.1.0.800039)

. . . continues on next page . . .

... continued from previous page ...

References
cve: CVE-2020-15466
url: https://www.wireshark.org/security/wnpa-sec-2020-09
cert-bund: WID-SEC-2023-1919
cert-bund: CB-K20/0655
dfn-cert: DFN-CERT-2023-1743
dfn-cert: DFN-CERT-2021-0257
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1734
dfn-cert: DFN-CERT-2020-1448

[return to 192.168.218.129]

2.1.3 Medium package

Medium (CVSS: 6.8)
NVT: Ubuntu: Security Advisory (USN-5589-1)

Summary
The remote host is missing an update for the 'linux, linux-raspi' package(s) announced via the USN-5589-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.125.126

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

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

Vulnerability Insight
Asaf Modelevsky discovered that the Intel(R) 10GbE PCI Express (ixgbe) Ethernet driver for the Linux kernel performed insufficient control flow management. A local attacker could possibly use this to cause a denial of service. (CVE-2021-33061)
It was discovered that the virtual terminal driver in the Linux kernel did not properly handle VGA console font changes, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-33656)

... 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-5589-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5589.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5589-1
cve: CVE-2021-33061
cve: CVE-2021-33656
advisory_id: USN-5589-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-0734
cert-bund: WID-SEC-2022-0320
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2174
dfn-cert: DFN-CERT-2022-2172
dfn-cert: DFN-CERT-2022-2102
dfn-cert: DFN-CERT-2022-2063
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2022-1930
dfn-cert: DFN-CERT-2022-1918
dfn-cert: DFN-CERT-2022-1906
dfn-cert: DFN-CERT-2022-1888
dfn-cert: DFN-CERT-2022-1879
dfn-cert: DFN-CERT-2022-1867
dfn-cert: DFN-CERT-2022-1866
dfn-cert: DFN-CERT-2022-1847
dfn-cert: DFN-CERT-2022-1823
dfn-cert: DFN-CERT-2022-1822
dfn-cert: DFN-CERT-2022-1795
dfn-cert: DFN-CERT-2022-1771
dfn-cert: DFN-CERT-2022-1768
dfn-cert: DFN-CERT-2022-1767
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1341

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.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: intel-microcode
Installed version: intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version: >=intel-microcode-3.20230214.0ubuntu0.20.04.1

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: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-5886-1
cve: CVE-2022-21216
cve: CVE-2022-33196
cve: CVE-2022-33972
cve: CVE-2022-38090
advisory_id: USN-5886-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0393
cert-bund: WID-SEC-2023-0377
dfn-cert: DFN-CERT-2023-2192
dfn-cert: DFN-CERT-2023-1166
dfn-cert: DFN-CERT-2023-0735
dfn-cert: DFN-CERT-2023-0412
dfn-cert: DFN-CERT-2023-0352

Medium (CVSS: 6.8)
NVT: Ubuntu: Security Advisory (USN-5486-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-5486-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: intel-microcode
Installed version: intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version: >=intel-microcode-3.20220510.0ubuntu0.20.04.1

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

Affected Software/OS
'intel-microcode' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that some Intel processors did not implement sufficient control flow management. A local attacker could use this to cause a denial of service. (CVE-2021-0127)
Joseph Nuzman discovered that some Intel processors did not properly initialise shared resources. A local attacker could use this to obtain sensitive information. (CVE-2021-0145)

... continues on next page ...

... continued from previous page ...

Mark Ermolov, Dmitry Sklyarov and Maxim Goryachy discovered that some Intel processors did not prevent test and debug logic from being activated at runtime. A local attacker could use this to escalate privileges. (CVE-2021-0146)
It was discovered that some Intel processors did not properly restrict access in some situations. A local attacker could use this to obtain sensitive information. (CVE-2021-33117)
Brandon Miller discovered that some Intel processors did not properly restrict access in some situations. A local attacker could use this to obtain sensitive information or a remote attacker could use this to cause a denial of service. (CVE-2021-33120)
It was discovered that some Intel processors did not completely perform cleanup actions on multi-core shared buffers. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21123, CVE-2022-21127)
Alysa Milburn, Jason Brandt, Avishai Redelman and Nir Lavi discovered that some Intel processors improperly optimised security-critical code. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21151)
It was discovered that some Intel processors did not properly perform cleanup during specific special register write operations. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21166)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5486-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5486.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5486-1`
`cve: CVE-2021-0127`
`cve: CVE-2021-0145`
`cve: CVE-2021-0146`
`cve: CVE-2021-33117`
`cve: CVE-2021-33120`
`cve: CVE-2022-21123`
`cve: CVE-2022-21127`
`cve: CVE-2022-21151`
`cve: CVE-2022-21166`
`advisory_id: USN-5486-1`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2022-1767`
`cert-bund: WID-SEC-2022-0392`
`cert-bund: WID-SEC-2022-0391`
`cert-bund: WID-SEC-2022-0390`
`cert-bund: WID-SEC-2022-0336`
`cert-bund: WID-SEC-2022-0330`
`cert-bund: WID-SEC-2022-0303`
`cert-bund: WID-SEC-2022-0176`

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0073
cert-bund: CB-K22/0586
cert-bund: CB-K22/0576
cert-bund: CB-K22/0567
cert-bund: CB-K22/0150
cert-bund: CB-K21/1174
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2858
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-1725
dfn-cert: DFN-CERT-2022-1664
dfn-cert: DFN-CERT-2022-1663
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1529
dfn-cert: DFN-CERT-2022-1523
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1413
dfn-cert: DFN-CERT-2022-1405
dfn-cert: DFN-CERT-2022-1378
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1365
dfn-cert: DFN-CERT-2022-1358
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1338
dfn-cert: DFN-CERT-2022-1336
dfn-cert: DFN-CERT-2022-1334
dfn-cert: DFN-CERT-2022-1333
dfn-cert: DFN-CERT-2022-1328
dfn-cert: DFN-CERT-2022-1141
dfn-cert: DFN-CERT-2022-1087
dfn-cert: DFN-CERT-2022-1043

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-0401
dfn-cert: DFN-CERT-2022-0326
dfn-cert: DFN-CERT-2022-0301
dfn-cert: DFN-CERT-2022-0299
dfn-cert: DFN-CERT-2021-2339

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory (USN-6286-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-6286-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: intel-microcode
Installed version: intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version: >=intel-microcode-3.20230808.0ubuntu0.20.04.1

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 23.04.

Vulnerability Insight
Daniel Moghimi discovered that some Intel(R) Processors did not properly clear microarchitectural state after speculative execution of various instructions. A local unprivileged user could use this to obtain to sensitive information. (CVE-2022-40982)
It was discovered that some Intel(R) Xeon(R) Processors did not properly restrict error injection for Intel(R) SGX or Intel(R) TDX. A local privileged user could use this to further escalate their privileges. (CVE-2022-41804)
It was discovered that some 3rd Generation Intel(R) Xeon(R) Scalable processors did not properly restrict access in some situations. A local privileged attacker could use this to obtain sensitive information. (CVE-2023-23908)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6286-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6286.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-6286-1
cve: CVE-2022-40982
cve: CVE-2022-41804
cve: CVE-2023-23908
advisory_id: USN-6286-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2007
cert-bund: WID-SEC-2023-2005
dfn-cert: DFN-CERT-2024-1399
dfn-cert: DFN-CERT-2024-1011
dfn-cert: DFN-CERT-2024-0661
dfn-cert: DFN-CERT-2024-0656
dfn-cert: DFN-CERT-2024-0281
dfn-cert: DFN-CERT-2024-0249
dfn-cert: DFN-CERT-2023-2986
dfn-cert: DFN-CERT-2023-2925
dfn-cert: DFN-CERT-2023-2915
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2342
dfn-cert: DFN-CERT-2023-2290
dfn-cert: DFN-CERT-2023-2210
dfn-cert: DFN-CERT-2023-2123
dfn-cert: DFN-CERT-2023-2112
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-2037
dfn-cert: DFN-CERT-2023-2009
dfn-cert: DFN-CERT-2023-2008
dfn-cert: DFN-CERT-2023-2007
dfn-cert: DFN-CERT-2023-2006
dfn-cert: DFN-CERT-2023-1968
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1885
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1866

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1864
dfn-cert: DFN-CERT-2023-1862
dfn-cert: DFN-CERT-2023-1859
dfn-cert: DFN-CERT-2023-1857
dfn-cert: DFN-CERT-2023-1849
dfn-cert: DFN-CERT-2023-1847
dfn-cert: DFN-CERT-2023-1841

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory (USN-5454-1)

Summary
The remote host is missing an update for the 'cups' package(s) announced via the USN-5454-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: cups
Installed version: cups-2.3.1-9ubuntu1.1
Fixed version: >=cups-2.3.1-9ubuntu1.2

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

Affected Software/OS
'cups' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Joshua Mason discovered that CUPS incorrectly handled the secret key used to access the administrative web interface. A remote attacker could possibly use this issue to open a session as an administrator and execute arbitrary code. (CVE-2022-26691)
It was discovered that CUPS incorrectly handled certain memory operations when handling IPP printing. A remote attacker could possibly use this issue to cause CUPS to crash, leading to a denial of service, or obtain sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2019-8842, CVE-2020-10001)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5454-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5454.1
Version used: 2024-02-02T04:09:01Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-5454-1
cve: CVE-2019-8842
cve: CVE-2020-10001
cve: CVE-2022-26691
advisory_id: USN-5454-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2022-0365
cert-bund: CB-K22/0654
cert-bund: CB-K21/0136
cert-bund: CB-K20/0845
cert-bund: CB-K19/1065
dfn-cert: DFN-CERT-2022-1600
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1234
dfn-cert: DFN-CERT-2022-1197
dfn-cert: DFN-CERT-2021-0227
dfn-cert: DFN-CERT-2021-0217
dfn-cert: DFN-CERT-2020-2726
dfn-cert: DFN-CERT-2020-1208
dfn-cert: DFN-CERT-2019-2621
```

Medium (CVSS: 6.6)
NVT: Ubuntu: Security Advisory (USN-5614-1)

Summary
The remote host is missing an update for the 'wayland' package(s) announced via the USN-5614-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libwayland-client0
Installed version:    libwayland-client0-1.18.0-1
Fixed version:      >=libwayland-client0-1.18.0-1ubuntu0.1
Vulnerable package:   libwayland-egl1
Installed version:    libwayland-egl1-1.18.0-1
Fixed version:      >=libwayland-egl1-1.18.0-1ubuntu0.1
Vulnerable package:   libwayland-server0
Installed version:    libwayland-server0-1.18.0-1
Fixed version:      >=libwayland-server0-1.18.0-1ubuntu0.1
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
It was discovered that Wayland incorrectly handled reference counting certain objects. An attacker could use this issue to cause Wayland to crash, resulting in 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-5614-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5614.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5614-1`
`cve: CVE-2021-3782`
`advisory_id: USN-5614-1`
`cert-bund: WID-SEC-2023-1238`
`dfn-cert: DFN-CERT-2022-2053`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5520-1)

Summary
The remote host is missing an update for the 'libhttp-daemon-perl' package(s) announced via the USN-5520-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libhttp-daemon-perl
Installed version:    libhttp-daemon-perl-6.06-1
Fixed version:      >=libhttp-daemon-perl-6.06-1ubuntu0.1
```

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

Affected Software/OS
'libhttp-daemon-perl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that HTTP-Daemon incorrectly handled certain crafted requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5520-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5520.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5520-1`
`cve: CVE-2022-31081`
`advisory_id: USN-5520-1`
`cert-bund: WID-SEC-2023-1140`
`cert-bund: WID-SEC-2023-1022`
`dfn-cert: DFN-CERT-2023-1009`
`dfn-cert: DFN-CERT-2022-1587`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6322-1)

Summary
The remote host is missing an update for the 'elfutils' package(s) announced via the USN-6322-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libdw1
Installed version:    libdw1-0.176-1.1build1
Fixed version:      >=libdw1-0.176-1.1ubuntu0.1
Vulnerable package:   libelf1
Installed version:    libelf1-0.176-1.1build1
Fixed version:      >=libelf1-0.176-1.1ubuntu0.1
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that elfutils incorrectly handled certain malformed files. If a user or automated system were tricked into processing a specially crafted file, elfutils could be made to crash or consume resources, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-16062, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7665)
It was discovered that elfutils incorrectly handled bounds checks in certain functions when processing malformed files. If a user or automated system were tricked into processing a specially crafted file, elfutils could be made to crash or consume resources, resulting in a denial of service. (CVE-2020-21047, CVE-2021-33294)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6322-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6322.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6322-1`
`cve: CVE-2018-16062`
`cve: CVE-2018-16403`
`cve: CVE-2018-18310`
`cve: CVE-2018-18520`
`cve: CVE-2018-18521`
`cve: CVE-2019-7149`
`cve: CVE-2019-7150`
`cve: CVE-2019-7665`
`cve: CVE-2020-21047`
`cve: CVE-2021-33294`
`advisory_id: USN-6322-1`
`cert-bund: WID-SEC-2022-0517`
`cert-bund: CB-K20/1049`
`cert-bund: CB-K19/0696`
`dfn-cert: DFN-CERT-2023-2253`
`dfn-cert: DFN-CERT-2023-2024`
`dfn-cert: DFN-CERT-2022-1699`
`dfn-cert: DFN-CERT-2021-2263`
`dfn-cert: DFN-CERT-2019-1636`
`dfn-cert: DFN-CERT-2019-1196`
`dfn-cert: DFN-CERT-2019-1159`
`dfn-cert: DFN-CERT-2019-0400`
`dfn-cert: DFN-CERT-2019-0343`
`dfn-cert: DFN-CERT-2018-2348`
`dfn-cert: DFN-CERT-2018-1865`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6467-2)

Summary
The remote host is missing an update for the 'krb5' package(s) announced via the USN-6467-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgssapi-krb5-2
Installed version:    libgssapi-krb5-2-1.17-6ubuntu4.1
Fixed version:      >=libgssapi-krb5-2-1.17-6ubuntu4.4
Vulnerable package:   libk5crypto3
Installed version:    libk5crypto3-1.17-6ubuntu4.1
Fixed version:      >=libk5crypto3-1.17-6ubuntu4.4
Vulnerable package:   libkrb5-3
Installed version:    libkrb5-3-1.17-6ubuntu4.1
Fixed version:      >=libkrb5-3-1.17-6ubuntu4.4
Vulnerable package:   libkrb5support0
Installed version:    libkrb5support0-1.17-6ubuntu4.1
Fixed version:      >=libkrb5support0-1.17-6ubuntu4.4
```

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

Affected Software/OS
'krb5' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
USN-6467-1 fixed a vulnerability in Kerberos. This update provides the corresponding update for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.04.
Original advisory details:
Robert Morris discovered that Kerberos did not properly handle memory access when processing RPC data through kadmind, which could lead to the freeing of uninitialized memory. An authenticated remote attacker could possibly use this issue to cause kadmind to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6467-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6467.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6467-2`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2023-36054
advisory_id: USN-6467-2
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2023-1973
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2774
dfn-cert: DFN-CERT-2023-1901

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5213-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5213-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libjavascriptcoregtk-4.0-18
Installed version: libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libjavascriptcoregtk-4.0-18-2.34.3-0ubuntu0.20.04.1
Vulnerable package: libwebkit2gtk-4.0-37
Installed version: libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version: >=libwebkit2gtk-4.0-37-2.34.3-0ubuntu0.20.04.1

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
A large number of 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-5213-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5213.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

```
url: https://ubuntu.com/security/notices/USN-5213-1
cve: CVE-2021-30887
cve: CVE-2021-30890
advisory_id: USN-5213-1
cert-bund: WID-SEC-2023-0804
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: CB-K21/1125
cert-bund: CB-K21/1122
cert-bund: CB-K21/1115
dfn-cert: DFN-CERT-2022-1051
dfn-cert: DFN-CERT-2022-0191
dfn-cert: DFN-CERT-2022-0190
dfn-cert: DFN-CERT-2022-0164
dfn-cert: DFN-CERT-2022-0154
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2021-2675
dfn-cert: DFN-CERT-2021-2660
dfn-cert: DFN-CERT-2021-2253
dfn-cert: DFN-CERT-2021-2234
dfn-cert: DFN-CERT-2021-2232
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5742-1)

Summary
The remote host is missing an update for the 'jbigkit' package(s) announced via the USN-5742-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libjbig0
Installed version:    libjbig0-2.1-3.1build1
Fixed version:      >=libjbig0-2.1-3.1ubuntu0.20.04.1
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that JBIG-KIT incorrectly handled decoding certain large image files. If a user or automated system using JBIG-KIT were tricked into opening a specially crafted file, 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-5742-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5742.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5742-1`
`cve: CVE-2017-9937`
`advisory_id: USN-5742-1`
`cert-bund: WID-SEC-2022-2169`
`dfn-cert: DFN-CERT-2022-2679`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5992-1)

Summary
The remote host is missing an update for the 'ldb' package(s) announced via the USN-5992-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libldb2
Installed version:    libldb2-2:2.0.10-0ubuntu0.20.04.3
Fixed version:      >=libldb2-2:2.4.4-0ubuntu0.20.04.2
```

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

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

Vulnerability Insight
Demi Marie Obenour discovered that ldb, when used with Samba, incorrectly handled certain confidential attribute values. A remote authenticated attacker could possibly use this issue to obtain certain sensitive information.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5992-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5992.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5992-1
cve: CVE-2023-0614
advisory_id: USN-5992-1
cert-bund: WID-SEC-2023-0796
dfn-cert: DFN-CERT-2023-0858
dfn-cert: DFN-CERT-2023-0857
dfn-cert: DFN-CERT-2023-0713
dfn-cert: DFN-CERT-2023-0707
```

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:    libnss3-2:3.49.1-1ubuntu1.5
Fixed version:      >=libnss3-2:3.98-0ubuntu0.20.04.1
```

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)

... continues on next page ...

... continued from previous page ...

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
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-2024-1248`
`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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: libnss3
Installed version: libnss3-2:3.49.1-1ubuntu1.5
Fixed version: >=libnss3-2:3.98-0ubuntu0.20.04.2

Solution:
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-2024-1248
cert-bund: WID-SEC-2024-0669
cert-bund: WID-SEC-2024-0045
cert-bund: WID-SEC-2023-3185
cert-bund: WID-SEC-2023-2787

... continues on next page ...

... continued from previous page ...

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-6273-1)

Summary
The remote host is missing an update for the 'poppler' package(s) announced via the USN-6273-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpoppler97
Installed version: libpoppler97-0.86.1-0ubuntu1
Fixed version: >=libpoppler97-0.86.1-0ubuntu1.2

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

Affected Software/OS
'poppler' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Jieyong Ma discovered that poppler incorrectly handled certain malformed PDF files. A remote attacker could possibly use this issue to cause poppler to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2022-27337)

... continues on next page ...

... continued from previous page ...

It was discovered that poppler incorrectly handled certain malformed PDF files. A remote attacker could possibly use this issue to cause poppler to crash, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-34872)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6273-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6273.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6273-1`
`cve: CVE-2022-27337`
`cve: CVE-2023-34872`
`advisory_id: USN-6273-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2023-1921`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2022-1311`
`cert-bund: CB-K22/0545`
`dfn-cert: DFN-CERT-2024-0491`
`dfn-cert: DFN-CERT-2023-2727`
`dfn-cert: DFN-CERT-2023-2694`
`dfn-cert: DFN-CERT-2023-1790`
`dfn-cert: DFN-CERT-2023-1675`
`dfn-cert: DFN-CERT-2023-1627`
`dfn-cert: DFN-CERT-2022-2123`
`dfn-cert: DFN-CERT-2022-1963`
`dfn-cert: DFN-CERT-2022-1642`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6299-1)

Summary
The remote host is missing an update for the 'poppler' package(s) announced via the USN-6299-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libpoppler97
Installed version:    libpoppler97-0.86.1-0ubuntu1
Fixed version:      >=libpoppler97-0.86.1-0ubuntu1.3
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
It was discovered that poppler incorrectly handled certain malformed PDF files. If a user or an automated system were tricked into opening a specially crafted PDF file, a remote attacker could possibly use this issue to cause a denial of service. (CVE-2020-36023, CVE-2020-36024)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6299-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6299.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6299-1`
`cve: CVE-2020-36023`
`cve: CVE-2020-36024`
`advisory_id: USN-6299-1`
`cert-bund: WID-SEC-2023-2051`
`dfn-cert: DFN-CERT-2024-1386`
`dfn-cert: DFN-CERT-2023-2967`
`dfn-cert: DFN-CERT-2023-2957`
`dfn-cert: DFN-CERT-2023-2726`
`dfn-cert: DFN-CERT-2023-2617`
`dfn-cert: DFN-CERT-2023-2404`
`dfn-cert: DFN-CERT-2023-2403`
`dfn-cert: DFN-CERT-2023-1882`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6377-1)

Summary
The remote host is missing an update for the 'libraw' package(s) announced via the USN-6377-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libraw19
Installed version:    libraw19-0.19.5-1ubuntu1
Fixed version:      >=libraw19-0.19.5-1ubuntu1.3
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'libraw' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that LibRaw incorrectly handled certain photo files. If a user o automated system were tricked into processing a specially crafted photo file, a remote attacker could possibly cause applications linked against LibRaw to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6377-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6377.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6377-1`
`cve: CVE-2020-22628`
`advisory_id: USN-6377-1`
`dfn-cert: DFN-CERT-2023-2098`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5795-1)

Summary
The remote host is missing an update for the 'net-snmp' package(s) announced via the USN-5795-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libsnmp35
Installed version:    libsnmp35-5.8+dfsg-2ubuntu2.3
Fixed version:      >=libsnmp35-5.8+dfsg-2ubuntu2.6
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that Net-SNMP incorrectly handled certain requests. A remote attacker could possibly use these issues to cause Net-SNMP to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5795-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5795.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5795-1`
`cve: CVE-2022-44792`
`cve: CVE-2022-44793`
`advisory_id: USN-5795-1`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1969`
`cert-bund: WID-SEC-2022-1996`
`cert-bund: WID-SEC-2022-1970`
`dfn-cert: DFN-CERT-2023-1230`
`dfn-cert: DFN-CERT-2023-1196`
`dfn-cert: DFN-CERT-2023-0062`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5053-1)

Summary
The remote host is missing an update for the 'libssh' package(s) announced via the USN-5053-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libssh-4
Installed version:    libssh-4-0.9.3-2ubuntu2.1
Fixed version:      >=libssh-4-0.9.3-2ubuntu2.2
```

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

Affected Software/OS
'libssh' package(s) on Ubuntu 20.04, Ubuntu 21.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that libssh incorrectly handled rekeying. A remote attacker could use this issue to cause libssh to crash, resulting in 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-5053-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5053.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5053-1`
`cve: CVE-2021-3634`
`advisory_id: USN-5053-1`
`cert-bund: WID-SEC-2022-0101`
`cert-bund: WID-SEC-2022-0001`
`cert-bund: CB-K22/0062`
`cert-bund: CB-K21/0918`
`dfn-cert: DFN-CERT-2024-0440`
`dfn-cert: DFN-CERT-2022-1304`
`dfn-cert: DFN-CERT-2022-1294`
`dfn-cert: DFN-CERT-2022-0118`
`dfn-cert: DFN-CERT-2021-1871`
`dfn-cert: DFN-CERT-2021-1823`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6138-1)

Summary
The remote host is missing an update for the 'libssh' package(s) announced via the USN-6138-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libssh-4
Installed version:    libssh-4-0.9.3-2ubuntu2.1
Fixed version:      >=libssh-4-0.9.3-2ubuntu2.3
```

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

Affected Software/OS
'libssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Philip Turnbull discovered that libssh incorrectly handled rekeying with algorithm guessing. A remote attacker could use this issue to cause libssh to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-1667)
Kevin Backhouse discovered that libssh incorrectly handled verifying data signatures. A remote attacker could possibly use this issue to bypass authorization. (CVE-2023-2283)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6138-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6138.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6138-1`
`cve: CVE-2023-1667`
`cve: CVE-2023-2283`
`advisory_id: USN-6138-1`
`cert-bund: WID-SEC-2024-0869`
`cert-bund: WID-SEC-2024-0119`
`cert-bund: WID-SEC-2024-0106`
`cert-bund: WID-SEC-2023-2679`
`cert-bund: WID-SEC-2023-2112`
`cert-bund: WID-SEC-2023-1159`
`dfn-cert: DFN-CERT-2024-0440`
`dfn-cert: DFN-CERT-2024-0267`
`dfn-cert: DFN-CERT-2024-0154`
`dfn-cert: DFN-CERT-2024-0127`
`dfn-cert: DFN-CERT-2023-1955`
`dfn-cert: DFN-CERT-2023-1939`
`dfn-cert: DFN-CERT-2023-1903`
`dfn-cert: DFN-CERT-2023-1228`
`dfn-cert: DFN-CERT-2023-1102`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6119-1)

Summary
The remote host is missing an update for the 'openssl, openssl1.0' package(s) announced via the USN-6119-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  libssl1.1`

... continues on next page ...

... continued from previous page ...

Installed version: libssl1.1-1.1.1f-1ubuntu2.4
Fixed version: >=libssl1.1-1.1.1f-1ubuntu2.19

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

Affected Software/OS
'openssl, openssl1.0' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Matt Caswell discovered that OpenSSL incorrectly handled certain ASN.1 object identifiers. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, resulting in a denial of service. (CVE-2023-2650)
Anton Romanov discovered that OpenSSL incorrectly handled AES-XTS cipher decryption on 64-bit ARM platforms. An 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, Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-1255)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6119-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6119.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6119-1
cve: CVE-2023-1255
cve: CVE-2023-2650
advisory_id: USN-6119-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0120
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2024-0053
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2690
cert-bund: WID-SEC-2023-2674
cert-bund: WID-SEC-2023-1794
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1323
cert-bund: WID-SEC-2023-1053
dfn-cert: DFN-CERT-2024-1067
dfn-cert: DFN-CERT-2024-0565
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2024-0125

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-3071
dfn-cert: DFN-CERT-2023-3070
dfn-cert: DFN-CERT-2023-2749
dfn-cert: DFN-CERT-2023-2545
dfn-cert: DFN-CERT-2023-2536
dfn-cert: DFN-CERT-2023-2116
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1642
dfn-cert: DFN-CERT-2023-1462
dfn-cert: DFN-CERT-2023-1428
dfn-cert: DFN-CERT-2023-1332
dfn-cert: DFN-CERT-2023-1246
dfn-cert: DFN-CERT-2023-1245
dfn-cert: DFN-CERT-2023-1233
dfn-cert: DFN-CERT-2023-0929
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6622-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-6622-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libssl1.1
Installed version:    libssl1.1-1.1.1f-1ubuntu2.4
Fixed version:      >=libssl1.1-1.1.1f-1ubuntu2.21
```

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

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

Vulnerability Insight
David Benjamin discovered that OpenSSL incorrectly handled excessively long X9.42 DH keys. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2023-5678)

... continues on next page ...

... continued from previous page ...

Sverker Eriksson discovered that OpenSSL incorrectly handled POLY1304 MAC on the PowerPC architecture. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-6129)
It was discovered that OpenSSL incorrectly handled excessively long RSA public keys. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-6237)
Bahaa Naamneh discovered that OpenSSL incorrectly handled certain malformed PKCS12 files. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2024-0727)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6622-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6622.1
Version used: `2024-02-06T04:08:43Z`

References
`url: https://ubuntu.com/security/notices/USN-6622-1`
`cve: CVE-2023-5678`
`cve: CVE-2023-6129`
`cve: CVE-2023-6237`
`cve: CVE-2024-0727`
`advisory_id: USN-6622-1`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-0894`
`cert-bund: WID-SEC-2024-0769`
`cert-bund: WID-SEC-2024-0181`
`cert-bund: WID-SEC-2024-0093`
`cert-bund: WID-SEC-2024-0034`
`cert-bund: WID-SEC-2023-2838`
`dfn-cert: DFN-CERT-2024-1413`
`dfn-cert: DFN-CERT-2024-1166`
`dfn-cert: DFN-CERT-2024-1067`
`dfn-cert: DFN-CERT-2024-1011`
`dfn-cert: DFN-CERT-2024-1002`
`dfn-cert: DFN-CERT-2024-0764`
`dfn-cert: DFN-CERT-2024-0732`
`dfn-cert: DFN-CERT-2024-0723`
`dfn-cert: DFN-CERT-2024-0722`
`dfn-cert: DFN-CERT-2024-0539`
`dfn-cert: DFN-CERT-2024-0531`
`dfn-cert: DFN-CERT-2024-0374`
`dfn-cert: DFN-CERT-2024-0296`
`dfn-cert: DFN-CERT-2024-0253`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0225
dfn-cert: DFN-CERT-2024-0191
dfn-cert: DFN-CERT-2024-0175
dfn-cert: DFN-CERT-2024-0106
dfn-cert: DFN-CERT-2024-0058
dfn-cert: DFN-CERT-2023-2960
dfn-cert: DFN-CERT-2023-2740

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5084-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5084-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.2

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

Affected Software/OS
'tiff' package(s) on Ubuntu 20.04.

Vulnerability Insight
It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5084-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5084.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5084-1
cve: CVE-2020-19143
advisory_id: USN-5084-1

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2022-0723
dfn-cert: DFN-CERT-2021-1973

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6290-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-6290-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.9

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 23.04.

Vulnerability Insight
It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files with the tiffcrop utility. 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. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-48281)
It was discovered that LibTIFF incorrectly handled certain image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 23.04. (CVE-2023-2731)
It was discovered that LibTIFF incorrectly handled certain image files with the tiffcp utility. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause tiffcp to crash, resulting in a denial of service. (CVE-2023-2908)
It was discovered that LibTIFF incorrectly handled certain file paths. If a user were tricked into specifying certain output paths, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-3316)
It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2023-3618)

... continues on next page ...

... continued from previous page ...

It was discovered that LibTIFF could be made to write out of bounds when processing certain malformed image files. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-25433, CVE-2023-26966)
It was discovered that LibTIFF did not properly managed memory when processing certain malformed image files with the tiffcrop utility. 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. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-26965)
It was discovered that LibTIFF contained an arithmetic overflow. If a user were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. (CVE-2023-38288, CVE-2023-38289)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6290-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6290.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6290-1`
`cve: CVE-2022-48281`
`cve: CVE-2023-25433`
`cve: CVE-2023-26965`
`cve: CVE-2023-26966`
`cve: CVE-2023-2731`
`cve: CVE-2023-2908`
`cve: CVE-2023-3316`
`cve: CVE-2023-3618`
`cve: CVE-2023-38288`
`cve: CVE-2023-38289`
`advisory_id: USN-6290-1`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1858`
`cert-bund: WID-SEC-2023-1613`
`cert-bund: WID-SEC-2023-1605`
`cert-bund: WID-SEC-2023-1514`
`cert-bund: WID-SEC-2023-1479`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1223`
`cert-bund: WID-SEC-2023-0170`
`dfn-cert: DFN-CERT-2024-1151`
`dfn-cert: DFN-CERT-2024-0781`
`dfn-cert: DFN-CERT-2024-0719`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-3122
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2769
dfn-cert: DFN-CERT-2023-2738
dfn-cert: DFN-CERT-2023-1893
dfn-cert: DFN-CERT-2023-1752
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2023-1608
dfn-cert: DFN-CERT-2023-1445
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0220
dfn-cert: DFN-CERT-2023-0218

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6512-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-6512-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.11

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.

Vulnerability Insight
It was discovered that LibTIFF could be made to run into an infinite loop. If a user or an automated system were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-40090)
It was discovered that LibTIFF could be made leak memory. If a user or an automated system were tricked into opening a specially crafted image file, an attacker could possibly use this issue to cause a denial of service. (CVE-2023-3576)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6512-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2023.6512.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6512-1
cve: CVE-2022-40090
cve: CVE-2023-3576
advisory_id: USN-6512-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2023-2187
cert-bund: WID-SEC-2023-1881
dfn-cert: DFN-CERT-2024-1151
dfn-cert: DFN-CERT-2024-0649
dfn-cert: DFN-CERT-2023-3122
dfn-cert: DFN-CERT-2023-2953
dfn-cert: DFN-CERT-2023-2769
dfn-cert: DFN-CERT-2023-2738

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6028-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-6028-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libxml2
Installed version: libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version: >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.6

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

Affected Software/OS
'libxml2' 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 lixml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2023-28484)
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash. (CVE-2023-29469)

... 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-6028-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6028.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6028-1`
`cve: CVE-2023-28484`
`cve: CVE-2023-29469`
`advisory_id: USN-6028-1`
`cert-bund: WID-SEC-2024-0119`
`cert-bund: WID-SEC-2023-2679`
`cert-bund: WID-SEC-2023-2674`
`cert-bund: WID-SEC-2023-2101`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1812`
`cert-bund: WID-SEC-2023-1794`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2023-0920`
`dfn-cert: DFN-CERT-2024-0232`
`dfn-cert: DFN-CERT-2024-0127`
`dfn-cert: DFN-CERT-2023-2545`
`dfn-cert: DFN-CERT-2023-2490`
`dfn-cert: DFN-CERT-2023-2194`
`dfn-cert: DFN-CERT-2023-1939`
`dfn-cert: DFN-CERT-2023-1895`
`dfn-cert: DFN-CERT-2023-1845`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-1642`
`dfn-cert: DFN-CERT-2023-0969`
`dfn-cert: DFN-CERT-2023-0836`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6417-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6417-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.164.161
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the eBPF implementation in the Linux kernel contained a race condition around read-only maps. A privileged attacker could use this to modify read-only maps. (CVE-2021-4001)
It was discovered that the IPv6 implementation in the Linux kernel contained a high rate of hash collisions in connection lookup table. A remote attacker could use this to cause a denial of service (excessive CPU consumption). (CVE-2023-1206)
Yang Lan discovered that the GFS2 file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious GFS2 image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2023-3212)
Davide Ornaghi discovered that the DECnet network protocol implementation in the Linux kernel contained a null pointer dereference vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. Please note that kernel support for the DECnet has been removed to resolve this CVE. (CVE-2023-3338)
It was discovered that the NFC implementation in the Linux kernel contained a use-after-free vulnerability when performing peer-to-peer communication in certain conditions. A privileged attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2023-3863)
It was discovered that the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-4194)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6417-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6417.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6417-1`
`cve: CVE-2021-4001`
`cve: CVE-2023-1206`

... continues on next page ...

... continued from previous page ...

cve: CVE-2023-3212
cve: CVE-2023-3338
cve: CVE-2023-3863
cve: CVE-2023-4194
advisory_id: USN-6417-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2023-2557
cert-bund: WID-SEC-2023-1971
cert-bund: WID-SEC-2023-1877
cert-bund: WID-SEC-2023-1678
cert-bund: WID-SEC-2023-1571
cert-bund: WID-SEC-2023-1564
cert-bund: CB-K21/1224
dfn-cert: DFN-CERT-2024-0143
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2024-0094
dfn-cert: DFN-CERT-2023-2995
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-2792
dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2722
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2685
dfn-cert: DFN-CERT-2023-2682
dfn-cert: DFN-CERT-2023-2591
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2580
dfn-cert: DFN-CERT-2023-2575
dfn-cert: DFN-CERT-2023-2574
dfn-cert: DFN-CERT-2023-2543
dfn-cert: DFN-CERT-2023-2507
dfn-cert: DFN-CERT-2023-2506
dfn-cert: DFN-CERT-2023-2497
dfn-cert: DFN-CERT-2023-2496
dfn-cert: DFN-CERT-2023-2482
dfn-cert: DFN-CERT-2023-2480
dfn-cert: DFN-CERT-2023-2466
dfn-cert: DFN-CERT-2023-2465
dfn-cert: DFN-CERT-2023-2464
dfn-cert: DFN-CERT-2023-2463
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2391
dfn-cert: DFN-CERT-2023-2390
dfn-cert: DFN-CERT-2023-2385
dfn-cert: DFN-CERT-2023-2290
dfn-cert: DFN-CERT-2023-2219
dfn-cert: DFN-CERT-2023-2218

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2214
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2210
dfn-cert: DFN-CERT-2023-2163
dfn-cert: DFN-CERT-2023-2162
dfn-cert: DFN-CERT-2023-2161
dfn-cert: DFN-CERT-2023-2103
dfn-cert: DFN-CERT-2023-2080
dfn-cert: DFN-CERT-2023-2068
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1873
dfn-cert: DFN-CERT-2023-1872
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1669
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1622
dfn-cert: DFN-CERT-2023-1610
dfn-cert: DFN-CERT-2023-1563
dfn-cert: DFN-CERT-2023-1541
dfn-cert: DFN-CERT-2022-0711
dfn-cert: DFN-CERT-2022-0318
dfn-cert: DFN-CERT-2022-0260
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0193
dfn-cert: DFN-CERT-2022-0060
dfn-cert: DFN-CERT-2022-0020
dfn-cert: DFN-CERT-2021-2480

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5993-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5993-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: samba
Installed version: samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version: >=samba-2:4.15.13+dfsg-0ubuntu0.20.04.2

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
Demi Marie Obenour discovered that the Samba LDAP server incorrectly handled certain confidential attribute values. A remote authenticated attacker could possibly use this issue to obtain certain sensitive information. (CVE-2023-0614)
Andrew Bartlett discovered that the Samba AD DC admin tool incorrectly sent passwords in cleartext. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-0922)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5993-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5993.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5993-1`
`cve: CVE-2023-0614`
`cve: CVE-2023-0922`
`advisory_id: USN-5993-1`
`cert-bund: WID-SEC-2023-0796`
`dfn-cert: DFN-CERT-2023-0858`
`dfn-cert: DFN-CERT-2023-0857`
`dfn-cert: DFN-CERT-2023-0713`
`dfn-cert: DFN-CERT-2023-0710`
`dfn-cert: DFN-CERT-2023-0707`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6425-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-6425-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
`Vulnerable package:  samba`
`Installed version:  samba-2:4.11.6+dfsg-0ubuntu1.9`

... continues on next page ...

... continued from previous page ...

Fixed version: >=samba-2:4.15.13+dfsg-0ubuntu0.20.04.6

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Sri Nagasubramanian discovered that the Samba acl_xattr VFS module incorrectly handled read-only files. When Samba is configured to ignore system ACLs, a remote attacker could possibly use this issue to truncate read-only files. (CVE-2023-4091)
Andrew Bartlett discovered that Samba incorrectly handled the DirSync control. A remote attacker with an RODC DC account could possibly use this issue to obtain all domain secrets. (CVE-2023-4154)
Andrew Bartlett discovered that Samba incorrectly handled the rpcecho development server. A remote attacker could possibly use this issue to cause Samba to stop responding, resulting in a denial of service. (CVE-2023-42669)
Kirin van der Veer discovered that Samba incorrectly handled certain RPC service listeners. A remote attacker could possibly use this issue to cause Samba to start multiple incompatible RPC listeners, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-42670)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6425-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6425.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6425-1
cve: CVE-2023-4091
cve: CVE-2023-4154
cve: CVE-2023-42669
cve: CVE-2023-42670
advisory_id: USN-6425-1
cert-bund: WID-SEC-2024-0523
cert-bund: WID-SEC-2023-2620
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2023-2700
dfn-cert: DFN-CERT-2023-2494
dfn-cert: DFN-CERT-2023-2462
dfn-cert: DFN-CERT-2023-2447
dfn-cert: DFN-CERT-2023-2443

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6425-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-6425-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   samba
Installed version:    samba-2:4.11.6+dfsg-0ubuntu1.9
Fixed version:      >=samba-2:4.15.13+dfsg-0ubuntu0.20.04.7
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6425-1 fixed vulnerabilities in Samba. Due to a build issue on Ubuntu 20.04 LTS, the update introduced regressions in macro handling and possibly other functionality.
This update fixes the problem. We apologize for the inconvenience.
Original advisory details:
Sri Nagasubramanian discovered that the Samba acl_xattr VFS module incorrectly handled read-only files. When Samba is configured to ignore system ACLs, a remote attacker could possibly use this issue to truncate read-only files. (CVE-2023-4091)
Andrew Bartlett discovered that Samba incorrectly handled the DirSync control. A remote attacker with an RODC DC account could possibly use this issue to obtain all domain secrets. (CVE-2023-4154)
Andrew Bartlett discovered that Samba incorrectly handled the rpcecho development server. A remote attacker could possibly use this issue to cause Samba to stop responding, resulting in a denial of service. (CVE-2023-42669)
Kirin van der Veer discovered that Samba incorrectly handled certain RPC service listeners. A remote attacker could possibly use this issue to cause Samba to start multiple incompatible RPC listeners, resulting in a denial of service. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 23.04. (CVE-2023-42670)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6425-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6425.2
Version used: `2024-02-02T04:09:01Z`

References

. . . continues on next page . . .

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6425-2
url: https://launchpad.net/bugs/2039031
cve: CVE-2023-4091
cve: CVE-2023-4154
cve: CVE-2023-42669
cve: CVE-2023-42670
advisory_id: USN-6425-2
cert-bund: WID-SEC-2024-0523
cert-bund: WID-SEC-2023-2620
dfn-cert: DFN-CERT-2024-1065
dfn-cert: DFN-CERT-2024-0839
dfn-cert: DFN-CERT-2023-2700
dfn-cert: DFN-CERT-2023-2494
dfn-cert: DFN-CERT-2023-2462
dfn-cert: DFN-CERT-2023-2447
dfn-cert: DFN-CERT-2023-2443
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5704-1)

Summary
The remote host is missing an update for the 'dbus' package(s) announced via the USN-5704-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   dbus
Installed version:    dbus-1.12.16-2ubuntu2.1
Fixed version:      >=dbus-1.12.16-2ubuntu2.3
Vulnerable package:   libdbus-1-3
Installed version:    libdbus-1-3-1.12.16-2ubuntu2.1
Fixed version:      >=libdbus-1-3-1.12.16-2ubuntu2.3
```

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

Affected Software/OS
'dbus' 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 DBus incorrectly handled messages with invalid type signatures. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service. (CVE-2022-42010)
It was discovered that DBus was incorrectly validating the length of arrays of fixed-length items. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service. (CVE-2022-42011)
It was discovered that DBus incorrectly handled the body DBus message with attached file descriptors. A local attacker could possibly use this issue to cause DBus to crash, resulting in a denial of service. (CVE-2022-42012)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5704-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5704.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5704-1`
`cve: CVE-2022-42010`
`cve: CVE-2022-42011`
`cve: CVE-2022-42012`
`advisory_id: USN-5704-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0296`
`cert-bund: WID-SEC-2022-1644`
`dfn-cert: DFN-CERT-2023-1162`
`dfn-cert: DFN-CERT-2023-0372`
`dfn-cert: DFN-CERT-2023-0278`
`dfn-cert: DFN-CERT-2022-2215`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5374-1)

Summary
The remote host is missing an update for the 'libarchive' package(s) announced via the USN-5374-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libarchive13
Installed version:    libarchive13-3.4.0-2ubuntu1
Fixed version:      >=libarchive13-3.4.0-2ubuntu1.2
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'libarchive' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that libarchive incorrectly handled certain archive files. An attacker could possibly use this issue to expose sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5374-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5374.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5374-1`
`cve: CVE-2022-26280`
`advisory_id: USN-5374-1`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2022-0066`
`cert-bund: CB-K22/0363`
`dfn-cert: DFN-CERT-2023-1162`
`dfn-cert: DFN-CERT-2022-1253`
`dfn-cert: DFN-CERT-2022-0800`

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6535-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-6535-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.21
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.21
Vulnerable package:   libcurl4
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.21
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Harry Sintonen discovered that curl incorrectly handled mixed case cookie domains. A remote attacker could possibly use this issue to set cookies that get sent to different and unrelated sites and domains. (CVE-2023-46218)
Maksymilian Arciemowicz discovered that curl incorrectly handled long file names when saving HSTS data. This could result in curl losing HSTS data, and subsequent requests to a site would be done without it, contrary to expectations. This issue only affected Ubuntu 23.04 and Ubuntu 23.10. (CVE-2023-46219)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6535-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6535.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6535-1
cve: CVE-2023-46218
cve: CVE-2023-46219
advisory_id: USN-6535-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0992
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2023-3060
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0869
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0732
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0230
dfn-cert: DFN-CERT-2023-3208
dfn-cert: DFN-CERT-2023-3086
dfn-cert: DFN-CERT-2023-3064
dfn-cert: DFN-CERT-2023-3047
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5503-1)

Summary
The remote host is missing an update for the 'gnupg2' package(s) announced via the USN-5503-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   gnupg
Installed version:    gnupg-2.2.19-3ubuntu2.1
Fixed version:      >=gnupg-2.2.19-3ubuntu2.2
Vulnerable package:   gpg
Installed version:    gpg-2.2.19-3ubuntu2.1
Fixed version:      >=gpg-2.2.19-3ubuntu2.2
```

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

Affected Software/OS
'gnupg2' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Demi Marie Obenour discovered that GnuPG incorrectly handled injection in the status message. A remote attacker could possibly use this issue to forge signatures.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5503-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5503.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5503-1
cve: CVE-2022-34903
advisory_id: USN-5503-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2022-1715
cert-bund: WID-SEC-2022-0511
dfn-cert: DFN-CERT-2023-1162
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1489
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5658-1)

Summary
The remote host is missing an update for the 'isc-dhcp' package(s) announced via the USN-5658-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   isc-dhcp-client
Installed version:    isc-dhcp-client-4.4.1-2.1ubuntu5.20.04.2
Fixed version:      >=isc-dhcp-client-4.4.1-2.1ubuntu5.20.04.4
```

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

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

Vulnerability Insight
It was discovered that DHCP incorrectly handled option reference counting. A remote attacker could possibly use this issue to cause DHCP servers to crash, resulting in a denial of service. (CVE-2022-2928)
It was discovered that DHCP incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause DHCP clients and servers to consume resources, leading to a denial of service. (CVE-2022-2929)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5658-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5658.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5658-1
cve: CVE-2022-2928
cve: CVE-2022-2929
advisory_id: USN-5658-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2022-1634
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2023-0372
dfn-cert: DFN-CERT-2022-2200
```

Medium (CVSS: 6.5)
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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libaprutil1
Installed version:    libaprutil1-1.6.1-4ubuntu2
Fixed version:      >=libaprutil1-1.6.1-4ubuntu2.1
```

Solution:
Solution type: VendorFix
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: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5870-1
cve: CVE-2022-25147
advisory_id: USN-5870-1
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0124
cert-bund: WID-SEC-2023-2679
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-1812
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0245
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2023-1297
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0548
dfn-cert: DFN-CERT-2023-0302

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-6430-1)

Summary
The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-6430-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libavcodec58
Installed version:    libavcodec58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavcodec58-7:4.2.7-0ubuntu0.1+esm2
Vulnerable package:   libavformat58
Installed version:    libavformat58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavformat58-7:4.2.7-0ubuntu0.1+esm2
Vulnerable package:   libavutil56
Installed version:    libavutil56-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavutil56-7:4.2.7-0ubuntu0.1+esm2
Vulnerable package:   libpostproc55
Installed version:    libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version:      >=libpostproc55-7:4.2.7-0ubuntu0.1+esm2
Vulnerable package:   libswresample3
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1+esm2
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1+esm2
```

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.

Vulnerability Insight
It was discovered that FFmpeg did not properly handle certain inputs in vf_lagfun.c, resulting in a buffer overflow vulnerability. An attacker could possibly use this issue to cause a denial of service via application crash. This issue only affected Ubuntu 20.04 LTS. (CVE-2020-22024)

... continues on next page ...

... continued from previous page ...

It was discovered that FFmpeg incorrectly managed memory in avienc.c, resulting in a memory leak. An attacker could possibly use this issue to cause a denial of service via application crash. (CVE-2020-22039)
It was discovered that FFmpeg incorrectly handled certain files due to a memory leak in frame.c. An attacker could possibly use this issue to cause a denial of service via application crash. This issue affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-22040)
It was discovered that FFmpeg incorrectly handled certain files due to a memory leak in fifo.c. An attacker could possibly use this issue to cause a denial of service via application crash. (CVE-2020-22043)
It was discovered that FFmpeg incorrectly handled certain files due to a memory leak in vf_tile.c. If a user or automated system were tricked into processing a specially crafted MOV file, an attacker could possibly use this issue to cause a denial of service. (CVE-2020-22051)
It was discovered that FFmpeg incorrectly handled certain MOV files in timecode.c, leading to an integer overflow. An attacker could possibly use this issue to cause a denial of service using a crafted MOV file. This issue only affected Ubuntu 16.04 LTS. (CVE-2021-28429)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6430-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6430.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6430-1`
`cve: CVE-2020-22024`
`cve: CVE-2020-22039`
`cve: CVE-2020-22040`
`cve: CVE-2020-22043`
`cve: CVE-2020-22051`
`cve: CVE-2021-28429`
`advisory_id: USN-6430-1`
`cert-bund: WID-SEC-2023-2053`
`cert-bund: WID-SEC-2023-0011`
`cert-bund: WID-SEC-2022-0210`
`cert-bund: CB-K21/0746`
`cert-bund: CB-K21/0599`
`dfn-cert: DFN-CERT-2023-2499`
`dfn-cert: DFN-CERT-2023-2319`
`dfn-cert: DFN-CERT-2021-1863`
`dfn-cert: DFN-CERT-2021-1502`

Medium (CVSS: 6.4)
NVT: Ubuntu: Security Advisory (USN-6796-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'tpm2-tss' package(s) announced via the USN-6796-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libtss2-esys0
Installed version:    libtss2-esys0-2.3.2-1
Fixed version:      >=libtss2-esys0-2.3.2-1ubuntu0.20.04.2
```

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

Affected Software/OS
'tpm2-tss' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Fergus Dall discovered that TPM2 Software Stack did not properly handle layer arrays. An attacker could possibly use this issue to cause TPM2 Software Stack to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-22745)
Jurgen Repp and Andreas Fuchs discovered that TPM2 Software Stack did not validate the quote data after deserialization. An attacker could generate an arbitrary quote and cause TPM2 Software Stack to have unknown behavior. (CVE-2024-29040)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6796-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6796.1
Version used: `2024-05-30T04:08:53Z`

References

```
url: https://ubuntu.com/security/notices/USN-6796-1
cve: CVE-2023-22745
cve: CVE-2024-29040
advisory_id: USN-6796-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2023-2853
dfn-cert: DFN-CERT-2024-1429
dfn-cert: DFN-CERT-2024-1267
dfn-cert: DFN-CERT-2024-1119
dfn-cert: DFN-CERT-2023-0257
```

Medium (CVSS: 6.4)
NVT: Ubuntu: Security Advisory (USN-5045-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5045-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.81.85
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Norbert Slusarek discovered that the CAN broadcast manager (bcm) protocol implementation in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2021-34693)
It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device initialization failure, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-3564)
It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device detach events, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2021-3573)
It was discovered that the NFC implementation in the Linux kernel did not properly handle failed connect events leading to a NULL pointer dereference. A local attacker could use this to cause a denial of service. (CVE-2021-3587)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5045-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5045.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5045-1`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2021-34693
cve: CVE-2021-3564
cve: CVE-2021-3573
cve: CVE-2021-3587
advisory_id: USN-5045-1
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-1698
cert-bund: WID-SEC-2022-1697
cert-bund: WID-SEC-2022-0515
cert-bund: CB-K21/0683
cert-bund: CB-K21/0656
cert-bund: CB-K21/0637
cert-bund: CB-K21/0622
dfn-cert: DFN-CERT-2022-2268
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0668
dfn-cert: DFN-CERT-2022-0439
dfn-cert: DFN-CERT-2022-0436
dfn-cert: DFN-CERT-2022-0425
dfn-cert: DFN-CERT-2022-0344
dfn-cert: DFN-CERT-2022-0343
dfn-cert: DFN-CERT-2022-0339
dfn-cert: DFN-CERT-2022-0338
dfn-cert: DFN-CERT-2022-0336
dfn-cert: DFN-CERT-2022-0334
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2279
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-2135
dfn-cert: DFN-CERT-2021-2134
dfn-cert: DFN-CERT-2021-2133
dfn-cert: DFN-CERT-2021-2132
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1971
dfn-cert: DFN-CERT-2021-1953
dfn-cert: DFN-CERT-2021-1903
dfn-cert: DFN-CERT-2021-1898
dfn-cert: DFN-CERT-2021-1895
dfn-cert: DFN-CERT-2021-1796
dfn-cert: DFN-CERT-2021-1767
dfn-cert: DFN-CERT-2021-1766
dfn-cert: DFN-CERT-2021-1728
dfn-cert: DFN-CERT-2021-1692
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1554

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1531
dfn-cert: DFN-CERT-2021-1530
dfn-cert: DFN-CERT-2021-1506
dfn-cert: DFN-CERT-2021-1491
dfn-cert: DFN-CERT-2021-1482
dfn-cert: DFN-CERT-2021-1480
dfn-cert: DFN-CERT-2021-1354
dfn-cert: DFN-CERT-2021-1353
dfn-cert: DFN-CERT-2021-1270

Medium (CVSS: 6.4)
NVT: Ubuntu: Security Advisory (USN-5163-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5163-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: linux-image-generic-5.4.0.77.80
Fixed version: >=linux-image-generic-5.4.0.91.95

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Ilja Van Sprundel discovered that the SCTP implementation in the Linux kernel did not properly perform size validations on incoming packets in some situations. An attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2021-3655)
It was discovered that the Option USB High Speed Mobile device driver in the Linux kernel did not properly handle error conditions. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-37159)

... continues on next page ...

... continued from previous page ...

It was discovered that the AMD Cryptographic Coprocessor (CCP) driver in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2021-3744, CVE-2021-3764)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5163-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.5163.1

Version used: `2024-02-02T04:09:01Z`

References

`url: https://ubuntu.com/security/notices/USN-5163-1`
`cve: CVE-2021-3655`
`cve: CVE-2021-37159`
`cve: CVE-2021-3744`
`cve: CVE-2021-3764`
`advisory_id: USN-5163-1`
`cert-bund: WID-SEC-2022-0515`
`cert-bund: WID-SEC-2022-0222`
`cert-bund: WID-SEC-2022-0214`
`cert-bund: WID-SEC-2022-0112`
`cert-bund: CB-K22/0274`
`cert-bund: CB-K21/0970`
`cert-bund: CB-K21/0796`
`cert-bund: CB-K21/0774`
`dfn-cert: DFN-CERT-2022-1453`
`dfn-cert: DFN-CERT-2022-1294`
`dfn-cert: DFN-CERT-2022-1057`
`dfn-cert: DFN-CERT-2022-0737`
`dfn-cert: DFN-CERT-2022-0557`
`dfn-cert: DFN-CERT-2022-0548`
`dfn-cert: DFN-CERT-2022-0512`
`dfn-cert: DFN-CERT-2021-2637`
`dfn-cert: DFN-CERT-2021-2568`
`dfn-cert: DFN-CERT-2021-2560`
`dfn-cert: DFN-CERT-2021-2551`
`dfn-cert: DFN-CERT-2021-2544`
`dfn-cert: DFN-CERT-2021-2538`
`dfn-cert: DFN-CERT-2021-2537`
`dfn-cert: DFN-CERT-2021-2517`
`dfn-cert: DFN-CERT-2021-2513`
`dfn-cert: DFN-CERT-2021-2512`
`dfn-cert: DFN-CERT-2021-2492`
`dfn-cert: DFN-CERT-2021-2491`
`dfn-cert: DFN-CERT-2021-2490`
`dfn-cert: DFN-CERT-2021-2489`
`dfn-cert: DFN-CERT-2021-2472`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2021-2465
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2385
dfn-cert: DFN-CERT-2021-2384
dfn-cert: DFN-CERT-2021-2342
dfn-cert: DFN-CERT-2021-2341
dfn-cert: DFN-CERT-2021-2321
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-2211
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2162
dfn-cert: DFN-CERT-2021-2150
dfn-cert: DFN-CERT-2021-2138
dfn-cert: DFN-CERT-2021-2137
dfn-cert: DFN-CERT-2021-2120
dfn-cert: DFN-CERT-2021-2106
dfn-cert: DFN-CERT-2021-2103
dfn-cert: DFN-CERT-2021-2032
dfn-cert: DFN-CERT-2021-2023
dfn-cert: DFN-CERT-2021-1993
dfn-cert: DFN-CERT-2021-1987
dfn-cert: DFN-CERT-2021-1986
```

Medium (CVSS: 6.3)
NVT: Ubuntu: Security Advisory (USN-6540-1)

Summary
The remote host is missing an update for the 'bluez' package(s) announced via the USN-6540-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   bluez
Installed version:    bluez-5.53-0ubuntu3.2
Fixed version:      >=bluez-5.53-0ubuntu3.7
Vulnerable package:   libbluetooth3
Installed version:    libbluetooth3-5.53-0ubuntu3.2
Fixed version:      >=libbluetooth3-5.53-0ubuntu3.7
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'bluez' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that BlueZ did not properly restrict non-bonded devices from injecting HID events into the input subsystem. This could allow a physically proximate attacker to inject keystrokes and execute arbitrary commands whilst the device is discoverable.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6540-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6540.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6540-1`
`cve: CVE-2023-45866`
`advisory_id: USN-6540-1`
`cert-bund: WID-SEC-2023-3095`
`cert-bund: WID-SEC-2023-3094`
`cert-bund: WID-SEC-2023-3086`
`cert-bund: WID-SEC-2023-3057`
`dfn-cert: DFN-CERT-2023-3092`
`dfn-cert: DFN-CERT-2023-3089`
`dfn-cert: DFN-CERT-2023-3058`
`dfn-cert: DFN-CERT-2023-3032`

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-5548-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-5548-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.10+dfsg-5ubuntu0.20.04.1
Fixed version:      >=libxml2-2.9.10+dfsg-5ubuntu0.20.04.4
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libxml2' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5548-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5548.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5548-1`
`cve: CVE-2016-3709`
`advisory_id: USN-5548-1`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2022-0869`
`dfn-cert: DFN-CERT-2023-2194`
`dfn-cert: DFN-CERT-2022-2512`
`dfn-cert: DFN-CERT-2022-2378`

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-6155-1)

Summary
The remote host is missing an update for the 'requests' package(s) announced via the USN-6155-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-requests
Installed version:    python3-requests-2.22.0-2ubuntu1
Fixed version:      >=python3-requests-2.22.0-2ubuntu1.1
```

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

Affected Software/OS
'requests' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Dennis Brinkrolf and Tobias Funke discovered that Requests incorrectly leaked Proxy-Authorization headers. A remote 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-6155-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6155.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6155-1`
`cve: CVE-2023-32681`
`advisory_id: USN-6155-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-1935`
`cert-bund: WID-SEC-2023-1682`
`cert-bund: WID-SEC-2023-1603`
`dfn-cert: DFN-CERT-2023-2873`
`dfn-cert: DFN-CERT-2023-2783`
`dfn-cert: DFN-CERT-2023-2238`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-1845`
`dfn-cert: DFN-CERT-2023-1192`

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-5013-1)

Summary
The remote host is missing an update for the 'systemd' package(s) announced via the USN-5013-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   systemd
Installed version:    systemd-245.4-4ubuntu3.7
Fixed version:      >=systemd-245.4-4ubuntu3.10
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'systemd' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04.

Vulnerability Insight
It was discovered that systemd incorrectly handled certain mount paths. A local attacker could possibly use this issue to cause systemd to crash, resulting in a denial of service. (CVE-2021-33910)
Mitchell Frank discovered that systemd incorrectly handled DHCP FORCERENEW packets. A remote attacker could possibly use this issue to reconfigure servers. (CVE-2020-13529)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5013-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5013.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5013-1`
`cve: CVE-2020-13529`
`cve: CVE-2021-33910`
`advisory_id: USN-5013-1`
`cert-bund: WID-SEC-2022-1660`
`cert-bund: CB-K21/0772`
`cert-bund: CB-K21/0448`
`dfn-cert: DFN-CERT-2021-2391`
`dfn-cert: DFN-CERT-2021-2141`
`dfn-cert: DFN-CERT-2021-1802`
`dfn-cert: DFN-CERT-2021-1728`
`dfn-cert: DFN-CERT-2021-1690`
`dfn-cert: DFN-CERT-2021-1608`
`dfn-cert: DFN-CERT-2021-1532`

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-6599-1)

Summary
The remote host is missing an update for the 'jinja2' package(s) announced via the USN-6599-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-jinja2
Installed version:    python3-jinja2-2.10.1-2
Fixed version:      >=python3-jinja2-2.10.1-2ubuntu0.2
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'jinja2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
Yeting Li discovered that Jinja incorrectly handled certain regex. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. (CVE-2020-28493)
It was discovered that Jinja incorrectly handled certain HTML passed with xmlatter filter. An attacker could inject arbitrary HTML attributes keys and values potentially leading to XSS. (CVE-2024-22195)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6599-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6599.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6599-1`
`cve: CVE-2020-28493`
`cve: CVE-2024-22195`
`advisory_id: USN-6599-1`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-1228`
`cert-bund: WID-SEC-2024-1003`
`cert-bund: WID-SEC-2024-0949`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2024-0522`
`dfn-cert: DFN-CERT-2024-1392`
`dfn-cert: DFN-CERT-2024-1380`
`dfn-cert: DFN-CERT-2024-1089`
`dfn-cert: DFN-CERT-2024-0905`
`dfn-cert: DFN-CERT-2024-0834`
`dfn-cert: DFN-CERT-2024-0598`
`dfn-cert: DFN-CERT-2024-0219`
`dfn-cert: DFN-CERT-2024-0099`
`dfn-cert: DFN-CERT-2021-2354`
`dfn-cert: DFN-CERT-2021-2350`
`dfn-cert: DFN-CERT-2021-1801`
`dfn-cert: DFN-CERT-2021-1061`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-0432

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-6428-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-6428-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.10

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 23.04.

Vulnerability Insight
It was discovered that LibTIFF could be made to read out of bounds when processing certain malformed image files with the tiffcrop utility. 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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6428-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6428.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6428-1
cve: CVE-2023-1916
advisory_id: USN-6428-1
cert-bund: WID-SEC-2023-0889
dfn-cert: DFN-CERT-2023-3122
dfn-cert: DFN-CERT-2023-2452

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-6598-1)

Summary
The remote host is missing an update for the 'paramiko' package(s) announced via the USN-6598-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-paramiko
Installed version:    python3-paramiko-2.6.0-2
Fixed version:      >=python3-paramiko-2.6.0-2ubuntu0.3
```

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

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

Vulnerability Insight
Fabian Baumer, Marcus Brinkmann, Jorg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6598-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6598.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6598-1
cve: CVE-2023-48795
advisory_id: USN-6598-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-1082
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0892
cert-bund: WID-SEC-2024-0889
cert-bund: WID-SEC-2024-0885
cert-bund: WID-SEC-2024-0874
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0578
cert-bund: WID-SEC-2024-0564
cert-bund: WID-SEC-2024-0523
cert-bund: WID-SEC-2023-3174
dfn-cert: DFN-CERT-2024-1443
dfn-cert: DFN-CERT-2024-1442
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440
dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175
```

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-6499-1)

Summary
The remote host is missing an update for the 'gnutls28' package(s) announced via the USN-6499-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libgnutls30
Installed version:    libgnutls30-3.6.13-2ubuntu1.3
Fixed version:      >=libgnutls30-3.6.13-2ubuntu1.9
```

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

Affected Software/OS
'gnutls28' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that GnuTLS had a timing side-channel when handling certain RSA-PSK key exchanges. A remote attacker could possibly use this issue to recover sensitive information.

... 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-6499-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6499.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6499-1`
`cve: CVE-2023-5981`
`advisory_id: USN-6499-1`
`cert-bund: WID-SEC-2023-2978`
`dfn-cert: DFN-CERT-2024-1072`
`dfn-cert: DFN-CERT-2024-0940`
`dfn-cert: DFN-CERT-2024-0744`
`dfn-cert: DFN-CERT-2024-0496`
`dfn-cert: DFN-CERT-2024-0205`
`dfn-cert: DFN-CERT-2023-3203`
`dfn-cert: DFN-CERT-2023-2860`

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-5351-1)

Summary
The remote host is missing an update for the 'paramiko' package(s) announced via the USN-5351-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-paramiko
Installed version:    python3-paramiko-2.6.0-2
Fixed version:      >=python3-paramiko-2.6.0-2ubuntu0.1
```

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

Affected Software/OS
'paramiko' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Jan Schejbal discovered that Paramiko incorrectly handled permissions when writing private key files. A local attacker could possibly use this issue to gain access to private keys.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5351-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5351.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5351-1
cve: CVE-2022-24302
advisory_id: USN-5351-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2022-2256
cert-bund: CB-K22/0659
dfn-cert: DFN-CERT-2022-2786
dfn-cert: DFN-CERT-2022-2782
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-0573

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-5055-1)

Summary
The remote host is missing an update for the 'grilo' package(s) announced via the USN-5055-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libgrilo-0.3-0
Installed version: libgrilo-0.3-0-0.3.12-1
Fixed version: >=libgrilo-0.3-0-0.3.12-1ubuntu0.1

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

Affected Software/OS
'grilo' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Michael Catanzaro discovered that grilo incorrectly handled certain TLS certificate verification. An attacker could possibly use this issue to MITM attacks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5055-1)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2021.5055.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5055-1
cve: CVE-2021-39365
advisory_id: USN-5055-1
cert-bund: WID-SEC-2022-1153
cert-bund: CB-K21/0899
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1817

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-6561-1)

Summary
The remote host is missing an update for the 'libssh' package(s) announced via the USN-6561-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssh-4
Installed version: libssh-4-0.9.3-2ubuntu2.1
Fixed version: >=libssh-4-0.9.3-2ubuntu2.4

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

Affected Software/OS
'libssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Fabian Baumer, Marcus Brinkmann, Jorg Schwenk discovered that the SSH protocol was vulnerable to a prefix truncation attack. If a remote attacker was able to intercept SSH communications, extension negotiation messages could be truncated, possibly leading to certain algorithms and features being downgraded. This issue is known as the Terrapin attack. This update adds protocol extensions to mitigate this issue.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6561-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6561.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

url: https://ubuntu.com/security/notices/USN-6561-1
cve: CVE-2023-48795
advisory_id: USN-6561-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-1082
cert-bund: WID-SEC-2024-0899
cert-bund: WID-SEC-2024-0892
cert-bund: WID-SEC-2024-0889
cert-bund: WID-SEC-2024-0885
cert-bund: WID-SEC-2024-0874
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2024-0578
cert-bund: WID-SEC-2024-0564
cert-bund: WID-SEC-2024-0523
cert-bund: WID-SEC-2023-3174
dfn-cert: DFN-CERT-2024-1443
dfn-cert: DFN-CERT-2024-1442
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-1373
dfn-cert: DFN-CERT-2024-1260
dfn-cert: DFN-CERT-2024-1259
dfn-cert: DFN-CERT-2024-1108
dfn-cert: DFN-CERT-2024-1061
dfn-cert: DFN-CERT-2024-1029
dfn-cert: DFN-CERT-2024-1003
dfn-cert: DFN-CERT-2024-1000
dfn-cert: DFN-CERT-2024-0896
dfn-cert: DFN-CERT-2024-0779
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0698
dfn-cert: DFN-CERT-2024-0633
dfn-cert: DFN-CERT-2024-0619
dfn-cert: DFN-CERT-2024-0618
dfn-cert: DFN-CERT-2024-0616
dfn-cert: DFN-CERT-2024-0597
dfn-cert: DFN-CERT-2024-0545
dfn-cert: DFN-CERT-2024-0526
dfn-cert: DFN-CERT-2024-0491
dfn-cert: DFN-CERT-2024-0451
dfn-cert: DFN-CERT-2024-0440

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-0420
dfn-cert: DFN-CERT-2024-0388
dfn-cert: DFN-CERT-2024-0343
dfn-cert: DFN-CERT-2024-0306
dfn-cert: DFN-CERT-2024-0299
dfn-cert: DFN-CERT-2024-0285
dfn-cert: DFN-CERT-2024-0267
dfn-cert: DFN-CERT-2024-0251
dfn-cert: DFN-CERT-2024-0215
dfn-cert: DFN-CERT-2024-0211
dfn-cert: DFN-CERT-2024-0164
dfn-cert: DFN-CERT-2024-0154
dfn-cert: DFN-CERT-2024-0101
dfn-cert: DFN-CERT-2024-0092
dfn-cert: DFN-CERT-2024-0088
dfn-cert: DFN-CERT-2024-0067
dfn-cert: DFN-CERT-2024-0063
dfn-cert: DFN-CERT-2024-0062
dfn-cert: DFN-CERT-2024-0024
dfn-cert: DFN-CERT-2024-0013
dfn-cert: DFN-CERT-2023-3219
dfn-cert: DFN-CERT-2023-3218
dfn-cert: DFN-CERT-2023-3210
dfn-cert: DFN-CERT-2023-3201
dfn-cert: DFN-CERT-2023-3200
dfn-cert: DFN-CERT-2023-3195
dfn-cert: DFN-CERT-2023-3193
dfn-cert: DFN-CERT-2023-3191
dfn-cert: DFN-CERT-2023-3185
dfn-cert: DFN-CERT-2023-3184
dfn-cert: DFN-CERT-2023-3183
dfn-cert: DFN-CERT-2023-3182
dfn-cert: DFN-CERT-2023-3175

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-6237-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-6237-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: curl
Installed version: curl-7.68.0-1ubuntu2.5

... continues on next page ...

... continued from previous page ...

```
Fixed version:      >=curl-7.68.0-1ubuntu2.19
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.19
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.19
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
Hiroki Kurosawa discovered that curl incorrectly handled validating certain certificate wildcards. A remote attacker could possibly use this issue to spoof certain website certificates using IDN hosts. (CVE-2023-28321)
Hiroki Kurosawa discovered that curl incorrectly handled callbacks when certain options are set by applications. This could cause applications using curl to misbehave, resulting in information disclosure, or a denial of service. (CVE-2023-28322)
It was discovered that curl incorrectly handled saving cookies to files. A local attacker could possibly use this issue to create or overwrite files. This issue only affected Ubuntu 22.10, and Ubuntu 23.04. (CVE-2023-32001)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6237-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6237.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6237-1
cve: CVE-2023-28321
cve: CVE-2023-28322
cve: CVE-2023-32001
advisory_id: USN-6237-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0556
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2101
cert-bund: WID-SEC-2023-1880
cert-bund: WID-SEC-2023-1789
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1237
dfn-cert: DFN-CERT-2024-0869
dfn-cert: DFN-CERT-2024-0573
dfn-cert: DFN-CERT-2024-0230
dfn-cert: DFN-CERT-2023-3208
dfn-cert: DFN-CERT-2023-2643
dfn-cert: DFN-CERT-2023-2475
dfn-cert: DFN-CERT-2023-1939
dfn-cert: DFN-CERT-2023-1903
dfn-cert: DFN-CERT-2023-1895
dfn-cert: DFN-CERT-2023-1845
dfn-cert: DFN-CERT-2023-1827
dfn-cert: DFN-CERT-2023-1700
dfn-cert: DFN-CERT-2023-1698
dfn-cert: DFN-CERT-2023-1691
dfn-cert: DFN-CERT-2023-1664
dfn-cert: DFN-CERT-2023-1659
dfn-cert: DFN-CERT-2023-1294
dfn-cert: DFN-CERT-2023-1143
dfn-cert: DFN-CERT-2023-1142
dfn-cert: DFN-CERT-2023-1141
dfn-cert: DFN-CERT-2023-1140

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-6376-1)

Summary
The remote host is missing an update for the 'c-ares' package(s) announced via the USN-6376-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libc-ares2
Installed version: libc-ares2-1.15.0-1build1
Fixed version: >=libc-ares2-1.15.0-1ubuntu0.4

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

Affected Software/OS
'c-ares' package(s) on Ubuntu 20.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that c-ares incorrectly parsed certain SOA replies. A remote attacker could possibly use this issue to cause c-res to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6376-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6376.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6376-1`
`cve: CVE-2020-22217`
`advisory_id: USN-6376-1`
`cert-bund: WID-SEC-2024-0218`
`dfn-cert: DFN-CERT-2023-2885`
`dfn-cert: DFN-CERT-2023-2170`

Medium (CVSS: 5.7)
NVT: Ubuntu: Security Advisory (USN-6809-1)

Summary
The remote host is missing an update for the 'bluez' package(s) announced via the USN-6809-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   bluez
Installed version:    bluez-5.53-0ubuntu3.2
Fixed version:      >=bluez-5.53-0ubuntu3.8
Vulnerable package:   libbluetooth3
Installed version:    libbluetooth3-5.53-0ubuntu3.2
Fixed version:      >=libbluetooth3-5.53-0ubuntu3.8
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that BlueZ could be made to dereference invalid memory. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-3563)
It was discovered that BlueZ could be made to write out of bounds. If a user were tricked into connecting to a malicious device, an attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-27349)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6809-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6809.1
Version used: `2024-06-06T04:07:45Z`

References
`url: https://ubuntu.com/security/notices/USN-6809-1`
`cve: CVE-2022-3563`
`cve: CVE-2023-27349`
`advisory_id: USN-6809-1`
`cert-bund: WID-SEC-2024-1020`
`cert-bund: WID-SEC-2022-1761`
`dfn-cert: DFN-CERT-2024-1485`
`dfn-cert: DFN-CERT-2023-1408`
`dfn-cert: DFN-CERT-2023-0202`

Medium (CVSS: 5.6)
NVT: Ubuntu: Security Advisory (USN-5034-1)

Summary
The remote host is missing an update for the 'c-ares' package(s) announced via the USN-5034-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libc-ares2
Installed version:    libc-ares2-1.15.0-1build1
Fixed version:      >=libc-ares2-1.15.0-1ubuntu0.1
```

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

Affected Software/OS
'c-ares' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
Philipp Jeitner and Haya Shulman discovered that c-ares incorrectly validated certain hostnames returned by DNS servers. A remote attacker could possibly use this issue to perform Domain Hijacking attacks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5034-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5034.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5034-1`
`cve: CVE-2021-3672`
`advisory_id: USN-5034-1`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2023-0856`
`cert-bund: WID-SEC-2022-0029`
`dfn-cert: DFN-CERT-2021-1988`
`dfn-cert: DFN-CERT-2021-1930`
`dfn-cert: DFN-CERT-2021-1826`
`dfn-cert: DFN-CERT-2021-1800`
`dfn-cert: DFN-CERT-2021-1756`
`dfn-cert: DFN-CERT-2021-1728`
`dfn-cert: DFN-CERT-2021-1693`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6128-1)

Summary
The remote host is missing an update for the 'cups' package(s) announced via the USN-6128-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   cups
Installed version:    cups-2.3.1-9ubuntu1.1
Fixed version:      >=cups-2.3.1-9ubuntu1.3
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'cups' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that CUPS incorrectly handled logging. A remote attacker could use this issue to cause CUPS to crash, resulting in 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-6128-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6128.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6128-1`
`cve: CVE-2023-32324`
`advisory_id: USN-6128-1`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1349`
`dfn-cert: DFN-CERT-2023-2770`
`dfn-cert: DFN-CERT-2023-1643`
`dfn-cert: DFN-CERT-2023-1258`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5612-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-5612-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   intel-microcode
Installed version:    intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version:      >=intel-microcode-3.20220809.0ubuntu0.20.04.1
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Pietro Borrello, Andreas Kogler, Martin Schwarzl, Daniel Gruss, Michael Schwarz and Moritz Lipp discovered that some Intel processors did not properly clear data between subsequent xAPIC MMIO reads. This could allow a local attacker to compromise SGX enclaves.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5612-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5612.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5612-1`
`cve: CVE-2022-21233`
`advisory_id: USN-5612-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1432`
`cert-bund: WID-SEC-2022-0986`
`dfn-cert: DFN-CERT-2023-0735`
`dfn-cert: DFN-CERT-2022-1787`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5226-1)

Summary
The remote host is missing an update for the 'systemd' package(s) announced via the USN-5226-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   systemd
Installed version:    systemd-245.4-4ubuntu3.7
Fixed version:      >=systemd-245.4-4ubuntu3.15
```

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

Affected Software/OS
'systemd' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that systemd-tmpfiles employed uncontrolled recursion when removing deeply nested directory hierarchies. A local attacker could exploit this to cause systemd-tmpfiles to crash or have other unspecified impacts.

... 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-5226-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5226.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5226-1`
`cve: CVE-2021-3997`
`advisory_id: USN-5226-1`
`cert-bund: WID-SEC-2022-2277`
`cert-bund: CB-K22/0020`
`dfn-cert: DFN-CERT-2022-0044`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5673-1)

Summary
The remote host is missing an update for the 'unzip' package(s) announced via the USN-5673-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   unzip
Installed version:    unzip-6.0-25ubuntu1
Fixed version:      >=unzip-6.0-25ubuntu1.1
```

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

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

Vulnerability Insight
It was discovered that unzip did not properly handle unicode strings under certain circumstances. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-4217)
It was discovered that unzip did not properly perform bounds checking while converting wide strings to local strings. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2022-0529, CVE-2022-0530)

... 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-5673-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5673.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5673-1`
`url: https://launchpad.net/bugs/1957077`
`cve: CVE-2021-4217`
`cve: CVE-2022-0529`
`cve: CVE-2022-0530`
`advisory_id: USN-5673-1`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-1057`
`cert-bund: WID-SEC-2022-0943`
`cert-bund: CB-K22/0619`
`dfn-cert: DFN-CERT-2022-2263`
`dfn-cert: DFN-CERT-2022-1757`
`dfn-cert: DFN-CERT-2022-1143`
`dfn-cert: DFN-CERT-2022-1116`
`dfn-cert: DFN-CERT-2022-1115`
`dfn-cert: DFN-CERT-2022-1114`

Medium (CVSS: 5.5)
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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   tar
Installed version:    tar-1.30+dfsg-7ubuntu0.20.04.1
Fixed version:      >=tar-1.30+dfsg-7ubuntu0.20.04.3
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'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: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5900-1`
`cve: CVE-2022-48303`
`advisory_id: USN-5900-1`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2023-2910`
`cert-bund: WID-SEC-2023-2031`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-0213`
`dfn-cert: DFN-CERT-2023-2818`
`dfn-cert: DFN-CERT-2023-1230`
`dfn-cert: DFN-CERT-2023-0404`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5279-1)

Summary
The remote host is missing an update for the 'util-linux' package(s) announced via the USN-5279-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   mount
Installed version:    mount-2.34-0.1ubuntu9.1
Fixed version:      >=mount-2.34-0.1ubuntu9.3
Vulnerable package:   util-linux
Installed version:    util-linux-2.34-0.1ubuntu9.1
Fixed version:      >=util-linux-2.34-0.1ubuntu9.3
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'util-linux' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that util-linux incorrectly handled unmounting FUSE filesystems. A local attacker could possibly use this issue to unmount FUSE filesystems belonging to other users.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5279-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5279.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5279-1`
`cve: CVE-2021-3995`
`cve: CVE-2021-3996`
`advisory_id: USN-5279-1`
`cert-bund: WID-SEC-2022-0279`
`dfn-cert: DFN-CERT-2022-0320`
`dfn-cert: DFN-CERT-2022-0180`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5524-1)

Summary
The remote host is missing an update for the 'harfbuzz' package(s) announced via the USN-5524-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libharfbuzz0b
Installed version:    libharfbuzz0b-2.6.4-1ubuntu4
Fixed version:      >=libharfbuzz0b-2.6.4-1ubuntu4.2
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that HarfBuzz incorrectly handled certain glyph sizes. A remote attacker could use this issue to cause HarfBuzz to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5524-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5524.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5524-1`
`cve: CVE-2022-33068`
`advisory_id: USN-5524-1`
`cert-bund: WID-SEC-2022-2052`
`dfn-cert: DFN-CERT-2022-1595`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6129-1)

Summary
The remote host is missing an update for the 'avahi' package(s) announced via the USN-6129-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   avahi-daemon
Installed version:    avahi-daemon-0.7-4ubuntu7
Fixed version:      >=avahi-daemon-0.7-4ubuntu7.2
```

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

Affected Software/OS
'avahi' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Avahi incorrectly handled certain DBus messages. A local attacker could possibly use this issue to cause Avahi to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6129-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2023.6129.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6129-1
cve: CVE-2023-1981
advisory_id: USN-6129-1
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-1071
dfn-cert: DFN-CERT-2023-2777
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-0941

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6827-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-6827-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libtiff5
Installed version: libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version: >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.13

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 23.10, Ubuntu 24.04.

Vulnerability Insight
It was discovered that LibTIFF incorrectly handled memory when performing certain cropping operations, leading to a heap buffer overflow. An attacker could 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-6827-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6827.1
Version used: 2024-06-12T04:07:57Z

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-6827-1
cve: CVE-2023-3164
advisory_id: USN-6827-1
cert-bund: WID-SEC-2023-1405
dfn-cert: DFN-CERT-2024-1458

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6640-1)

Summary
The remote host is missing an update for the 'shadow' package(s) announced via the USN-6640-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   login
Installed version:    login-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=login-1:4.8.1-1ubuntu5.20.04.5
Vulnerable package:   passwd
Installed version:    passwd-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=passwd-1:4.8.1-1ubuntu5.20.04.5
```

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

Affected Software/OS
'shadow' 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 shadow was not properly sanitizing memory when running the password utility. An attacker could possibly use this issue to retrieve a password from memory, exposing sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6640-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6640.1
Version used: 2024-02-16T04:08:40Z

References

... continues on next page ...

... continued from previous page ...

```
url: https://ubuntu.com/security/notices/USN-6640-1
cve: CVE-2023-4641
advisory_id: USN-6640-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-3146
cert-bund: WID-SEC-2023-2357
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-0818
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-2141
```

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.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version:      >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.8
```

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)

... 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-5923-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5923.1
Version used: `2024-02-02T04:09:01Z`

References
`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-2023-1424`
`cert-bund: WID-SEC-2023-0350`
`dfn-cert: DFN-CERT-2023-2294`
`dfn-cert: DFN-CERT-2023-1996`
`dfn-cert: DFN-CERT-2023-1445`
`dfn-cert: DFN-CERT-2023-0884`
`dfn-cert: DFN-CERT-2023-0458`
`dfn-cert: DFN-CERT-2023-0426`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5762-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-5762-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   binutils
Installed version:    binutils-2.34-6ubuntu1.1
Fixed version:      >=binutils-2.34-6ubuntu1.4
```

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

... continues on next page ...

... continued from previous page ...

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

Vulnerability Insight
It was discovered that GNU binutils incorrectly handled certain COFF files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5762-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5762.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5762-1`
`cve: CVE-2022-38533`
`advisory_id: USN-5762-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2022-1192`
`dfn-cert: DFN-CERT-2023-3082`
`dfn-cert: DFN-CERT-2022-2757`
`dfn-cert: DFN-CERT-2022-2655`
`dfn-cert: DFN-CERT-2022-2427`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5523-2)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5523-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.1.0+git191117-2ubuntu0.20.04.1
Fixed version:      >=libtiff5-4.1.0+git191117-2ubuntu0.20.04.4
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
USN-5523-1 fixed several vulnerabilities in LibTIFF. This update provides the fixes for CVE-2022-0907, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924 and CVE-2022-22844 for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.
Original advisory details:
It was discovered that LibTIFF was not properly perf orming checks to guarantee that allocated memory space existed, which could lead to a NULL pointer dereference via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0907, CVE-2022-0908)
It was discovered that LibTIFF was not properly performing checks to avoid division calculations where the denominator value was zero, which could lead to an undefined behavior situation via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-0909)
It was discovered that LibTIFF was not properly performing bounds checks, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2022-0924)
It was discovered that LibTIFF was not properly performing the calculation of data that would eventually be used as a reference for bounds checking operations, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2020-19131)
It was discovered that LibTIFF was not properly terminating a function execution when processing incorrect data, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2020-19144)
It was discovered that LibTIFF was not properly performing checks when setting the value for data later used as reference during memory access, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information. (CVE-2022-22844)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5523-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5523.2
Version used: `2024-02-28T10:02:42Z`

References
`url: https://ubuntu.com/security/notices/USN-5523-2`
`cve: CVE-2022-0907`
`cve: CVE-2022-0908`
`cve: CVE-2022-0909`
`cve: CVE-2022-0924`
`cve: CVE-2022-22844`
`advisory_id: USN-5523-2`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2022-0730`
`cert-bund: WID-SEC-2022-0728`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-2592
dfn-cert: DFN-CERT-2022-2494
dfn-cert: DFN-CERT-2022-1601
dfn-cert: DFN-CERT-2022-1109
dfn-cert: DFN-CERT-2022-0682
dfn-cert: DFN-CERT-2022-0641
dfn-cert: DFN-CERT-2022-0504
dfn-cert: DFN-CERT-2022-0389
dfn-cert: DFN-CERT-2022-0166

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5008-1)

Summary
The remote host is missing an update for the 'avahi' package(s) announced via the USN-5008-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   avahi-daemon
Installed version:    avahi-daemon-0.7-4ubuntu7
Fixed version:      >=avahi-daemon-0.7-4ubuntu7.1
Vulnerable package:   libavahi-core7
Installed version:    libavahi-core7-0.7-4ubuntu7
Fixed version:      >=libavahi-core7-0.7-4ubuntu7.1
```

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

Affected Software/OS
'avahi' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04.

Vulnerability Insight
Thomas Kremer discovered that Avahi incorrectly handled termination signals on the Unix socket. A local attacker could possibly use this issue to cause Avahi to hang, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 20.10. (CVE-2021-3468)
It was discovered that Avahi incorrectly handled certain hostnames. A local attacker could possibly use this issue to cause Avahi to crash, resulting in a denial of service. This issue only affected Ubuntu 20.10 and Ubuntu 21.04. (CVE-2021-3502)

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-5008-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5008.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5008-1
cve: CVE-2021-3468
cve: CVE-2021-3502
advisory_id: USN-5008-1
cert-bund: WID-SEC-2022-0143
cert-bund: CB-K21/0608
dfn-cert: DFN-CERT-2023-3156
dfn-cert: DFN-CERT-2023-2777
dfn-cert: DFN-CERT-2021-1549
dfn-cert: DFN-CERT-2021-1457
dfn-cert: DFN-CERT-2021-1211
dfn-cert: DFN-CERT-2021-0945

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5329-1)

Summary
The remote host is missing an update for the 'tar' package(s) announced via the USN-5329-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: tar
Installed version: tar-1.30+dfsg-7ubuntu0.20.04.1
Fixed version: >=tar-1.30+dfsg-7ubuntu0.20.04.2

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

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

Vulnerability Insight
It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to cause tar to crash, resulting in a denial of service.

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-5329-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5329.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5329-1
cve: CVE-2021-20193
advisory_id: USN-5329-1
cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2023-0630
dfn-cert: DFN-CERT-2023-0553
dfn-cert: DFN-CERT-2022-1014
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-0644

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5395-1)

Summary
The remote host is missing an update for the 'networkd-dispatcher' package(s) announced via the USN-5395-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: networkd-dispatcher
Installed version: networkd-dispatcher-2.0.1-1
Fixed version: >=networkd-dispatcher-2.1-2~ubuntu20.04.2

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

Affected Software/OS
'networkd-dispatcher' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
It was discovered that networkd-dispatcher incorrectly handled internal scripts. A local attacker could possibly use this issue to cause a race condition, escalate privileges and execute arbitrary code. (CVE-2022-29799, CVE-2022-29800)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5395-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5395.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5395-1
cve: CVE-2022-29799
cve: CVE-2022-29800
advisory_id: USN-5395-1
cert-bund: CB-K22/0502
dfn-cert: DFN-CERT-2022-0953

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5395-2)

Summary
The remote host is missing an update for the 'networkd-dispatcher' package(s) announced via the USN-5395-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: networkd-dispatcher
Installed version: networkd-dispatcher-2.0.1-1
Fixed version: >=networkd-dispatcher-2.1-2~ubuntu20.04.3

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

Affected Software/OS
'networkd-dispatcher' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
USN-5395-1 fixed vulnerabilities in networkd-dispatcher. 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 networkd-dispatcher incorrectly handled internal scripts. A local attacker could possibly use this issue to cause a race condition, escalate privileges and execute arbitrary code. (CVE-2022-29799, CVE-2022-29800)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5395-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5395.2
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References
url: https://ubuntu.com/security/notices/USN-5395-2
url: https://launchpad.net/bugs/1971550
cve: CVE-2022-29799
cve: CVE-2022-29800
advisory_id: USN-5395-2
cert-bund: CB-K22/0502
dfn-cert: DFN-CERT-2022-0953

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5043-1)

Summary
The remote host is missing an update for the 'exiv2' package(s) announced via the USN-5043-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libexiv2-27
Installed version: libexiv2-27-0.27.2-8ubuntu2.4
Fixed version: >=libexiv2-27-0.27.2-8ubuntu2.6

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

Affected Software/OS
'exiv2' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-32815, CVE-2021-34334, CVE-2021-37620, CVE-2021-37622)
It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. These issues only affected Ubuntu 20.04 LTS and Ubuntu 21.04. (CVE-2021-34335, CVE-2021-37615, CVE-2021-37616, CVE-2021-37618, CVE-2021-37619, CVE-2021-37621, CVE-2021-37623)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5043-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5043.1
Version used: 2024-02-02T04:09:01Z

... continues on next page ...

... continued from previous page ...

References

```
url: https://ubuntu.com/security/notices/USN-5043-1
cve: CVE-2021-32815
cve: CVE-2021-34334
cve: CVE-2021-34335
cve: CVE-2021-37615
cve: CVE-2021-37616
cve: CVE-2021-37618
cve: CVE-2021-37619
cve: CVE-2021-37620
cve: CVE-2021-37621
cve: CVE-2021-37622
cve: CVE-2021-37623
advisory_id: USN-5043-1
cert-bund: WID-SEC-2022-1968
cert-bund: CB-K21/1196
dfn-cert: DFN-CERT-2023-0048
dfn-cert: DFN-CERT-2022-2697
dfn-cert: DFN-CERT-2022-2670
dfn-cert: DFN-CERT-2022-2492
dfn-cert: DFN-CERT-2022-2491
dfn-cert: DFN-CERT-2022-2290
dfn-cert: DFN-CERT-2021-2357
dfn-cert: DFN-CERT-2021-1733
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6297-1)

Summary

The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-6297-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   ghostscript
Installed version:    ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version:      >=ghostscript-9.50~dfsg-5ubuntu4.9
Vulnerable package:   libgs9
Installed version:    libgs9-9.50~dfsg-5ubuntu4.2
Fixed version:      >=libgs9-9.50~dfsg-5ubuntu4.9
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'ghostscript' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled outputting certain PDF files. A local attacker could potentially use this issue to cause a crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6297-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6297.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6297-1`
`cve: CVE-2023-38559`
`advisory_id: USN-6297-1`
`cert-bund: WID-SEC-2023-1968`
`dfn-cert: DFN-CERT-2024-0174`
`dfn-cert: DFN-CERT-2023-2877`
`dfn-cert: DFN-CERT-2023-2767`
`dfn-cert: DFN-CERT-2023-1807`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6266-1)

Summary
The remote host is missing an update for the 'librsvg' package(s) announced via the USN-6266-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   librsvg2-2
Installed version:    librsvg2-2-2.48.9-1ubuntu0.20.04.1
Fixed version:      >=librsvg2-2-2.48.9-1ubuntu0.20.04.4
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'librsvg' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Zac Sims discovered that librsvg incorrectly handled decoding URLs. A remote attacker could possibly use this issue to read arbitrary files by using an include element.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6266-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6266.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6266-1`
`cve: CVE-2023-38633`
`advisory_id: USN-6266-1`
`cert-bund: WID-SEC-2023-2902`
`cert-bund: WID-SEC-2023-1859`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-1735`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5026-1)

Summary
The remote host is missing an update for the 'qpdf' package(s) announced via the USN-5026-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libqpdf26
Installed version:    libqpdf26-9.1.1-1build1
Fixed version:      >=libqpdf26-9.1.1-1ubuntu0.1
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to consume resources, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-18020)
It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36978)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5026-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5026.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5026-1`
`cve: CVE-2018-18020`
`cve: CVE-2021-36978`
`advisory_id: USN-5026-1`
`dfn-cert: DFN-CERT-2023-2011`
`dfn-cert: DFN-CERT-2022-2001`
`dfn-cert: DFN-CERT-2022-1742`
`dfn-cert: DFN-CERT-2021-1625`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5224-1)

Summary
The remote host is missing an update for the 'ghostscript' package(s) announced via the USN-5224-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ghostscript
Installed version:    ghostscript-9.50~dfsg-5ubuntu4.2
Fixed version:      >=ghostscript-9.50~dfsg-5ubuntu4.5
Vulnerable package:   libgs9
Installed version:    libgs9-9.50~dfsg-5ubuntu4.2
Fixed version:      >=libgs9-9.50~dfsg-5ubuntu4.5
```

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

Affected Software/OS

... continues on next page ...

... continued from previous page ...

'ghostscript' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to cause Ghostscript to crash, resulting in 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-5224-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5224.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5224-1`
`cve: CVE-2021-45944`
`cve: CVE-2021-45949`
`advisory_id: USN-5224-1`
`cert-bund: WID-SEC-2023-0232`
`dfn-cert: DFN-CERT-2022-0653`
`dfn-cert: DFN-CERT-2022-0068`
`dfn-cert: DFN-CERT-2022-0034`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5043-2)

Summary
The remote host is missing an update for the 'exiv2' package(s) announced via the USN-5043-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libexiv2-27
Installed version:    libexiv2-27-0.27.2-8ubuntu2.4
Fixed version:      >=libexiv2-27-0.27.2-8ubuntu2.7
```

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

Affected Software/OS
'exiv2' package(s) on Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
USN-5043-1 fixed vulnerabilities in Exiv2. The update introduced a new regression that could cause a crash in applications using libexiv2. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-37620)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5043-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5043.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5043-2`
`url: https://launchpad.net/bugs/1941752`
`cve: CVE-2021-37620`
`advisory_id: USN-5043-2`
`dfn-cert: DFN-CERT-2023-0048`
`dfn-cert: DFN-CERT-2022-2697`
`dfn-cert: DFN-CERT-2022-2491`
`dfn-cert: DFN-CERT-2022-2290`
`dfn-cert: DFN-CERT-2021-1733`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5124-1)

Summary
The remote host is missing an update for the 'binutils' package(s) announced via the USN-5124-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   binutils
Installed version:    binutils-2.34-6ubuntu1.1
Fixed version:      >=binutils-2.34-6ubuntu1.3
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that GNU binutils incorrectly handled certain hash lookups. An attacker could use this issue to cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-16592)
It was discovered that GNU binutils incorrectly handled certain corrupt DWARF debug sections. An attacker could possibly use this issue to cause GNU binutils to consume memory, resulting in a denial of service. (CVE-2021-3487)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5124-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5124.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5124-1`
`cve: CVE-2020-16592`
`cve: CVE-2021-3487`
`advisory_id: USN-5124-1`
`cert-bund: WID-SEC-2022-1107`
`dfn-cert: DFN-CERT-2022-0661`
`dfn-cert: DFN-CERT-2022-0566`
`dfn-cert: DFN-CERT-2021-2413`
`dfn-cert: DFN-CERT-2021-2375`
`dfn-cert: DFN-CERT-2021-2311`
`dfn-cert: DFN-CERT-2021-2278`
`dfn-cert: DFN-CERT-2021-2229`
`dfn-cert: DFN-CERT-2021-1825`
`dfn-cert: DFN-CERT-2021-0742`
`dfn-cert: DFN-CERT-2020-2779`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6487-1)

Summary
The remote host is missing an update for the 'avahi' package(s) announced via the USN-6487-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   avahi-daemon
Installed version:    avahi-daemon-0.7-4ubuntu7
Fixed version:      >=avahi-daemon-0.7-4ubuntu7.3
Vulnerable package:   libavahi-client3
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    libavahi-client3-0.7-4ubuntu7
Fixed version:      >=libavahi-client3-0.7-4ubuntu7.3
Vulnerable package:   libavahi-common3
Installed version:    libavahi-common3-0.7-4ubuntu7
Fixed version:      >=libavahi-common3-0.7-4ubuntu7.3
Vulnerable package:   libavahi-core7
Installed version:    libavahi-core7-0.7-4ubuntu7
Fixed version:      >=libavahi-core7-0.7-4ubuntu7.3
```

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

Affected Software/OS
'avahi' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Evgeny Vereshchagin discovered that Avahi contained several reachable assertions, which could lead to intentional assertion failures when specially crafted user input was given. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-38469, CVE-2023-38470, CVE-2023-38471, CVE-2023-38472, CVE-2023-38473)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6487-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6487.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-6487-1
cve: CVE-2023-38469
cve: CVE-2023-38470
cve: CVE-2023-38471
cve: CVE-2023-38472
cve: CVE-2023-38473
advisory_id: USN-6487-1
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2023-2589
cert-bund: WID-SEC-2023-2023
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1215
dfn-cert: DFN-CERT-2024-0827
dfn-cert: DFN-CERT-2023-3179
dfn-cert: DFN-CERT-2023-3156
dfn-cert: DFN-CERT-2023-2938
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2918
dfn-cert: DFN-CERT-2023-2903

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6588-1)

Summary
The remote host is missing an update for the 'pam' package(s) announced via the USN-6588-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpam-modules
Installed version: libpam-modules-1.3.1-5ubuntu4.2
Fixed version: >=libpam-modules-1.3.1-5ubuntu4.7

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

Affected Software/OS
'pam' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Matthias Gerstner discovered that the PAM pam_namespace module incorrectly handled special files when performing directory checks. A local attacker could possibly use this issue to cause PAM to stop responding, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6588-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6588.1
Version used: 2024-02-14T04:08:59Z

References
url: https://ubuntu.com/security/notices/USN-6588-1
cve: CVE-2024-22365
advisory_id: USN-6588-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0995
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-0146

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6361-1)

Summary
The remote host is missing an update for the 'cups' package(s) announced via the USN-6361-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   cups
Installed version:    cups-2.3.1-9ubuntu1.1
Fixed version:      >=cups-2.3.1-9ubuntu1.5
```

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

Affected Software/OS
'cups' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that CUPS incorrectly authenticated certain remote requests. A remote attacker could possibly use this issue to obtain recently printed documents.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6361-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6361.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6361-1
cve: CVE-2023-32360
advisory_id: USN-6361-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2028
cert-bund: WID-SEC-2023-1251
dfn-cert: DFN-CERT-2023-2231
dfn-cert: DFN-CERT-2023-2229
dfn-cert: DFN-CERT-2023-2001
dfn-cert: DFN-CERT-2023-1156
dfn-cert: DFN-CERT-2023-1155
dfn-cert: DFN-CERT-2023-1154
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5733-1)

Summary
The remote host is missing an update for the 'flac' package(s) announced via the USN-5733-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libflac8
Installed version:    libflac8-1.3.3-1build1
Fixed version:      >=libflac8-1.3.3-1ubuntu0.1
```

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

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

Vulnerability Insight
It was discovered that FLAC was not properly performing memory management operations, which could result in a memory leak. An attacker could possibly use this issue to cause FLAC to consume resources, leading to a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. (CVE-2017-6888)
It was discovered that FLAC was not properly performing bounds checking operations when decoding data. If a user or automated system were tricked into processing a specially crafted file, an attacker could possibly use this issue to expose sensitive information or to cause FLAC to crash, leading to a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-0499)
It was discovered that FLAC was not properly performing bounds checking operations when encoding data. If a user or automated system were tricked into processing a specially crafted file, an attacker could possibly use this issue to expose sensitive information or to cause FLAC to crash, leading to a denial of service. (CVE-2021-0561)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5733-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5733.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5733-1
cve: CVE-2017-6888
cve: CVE-2020-0499
cve: CVE-2021-0561
```

... continues on next page ...

... continued from previous page ...

```
advisory_id: USN-5733-1
cert-bund: WID-SEC-2022-2387
cert-bund: WID-SEC-2022-2047
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: CB-K21/0615
cert-bund: CB-K20/1240
dfn-cert: DFN-CERT-2022-2923
dfn-cert: DFN-CERT-2022-2653
dfn-cert: DFN-CERT-2022-1143
dfn-cert: DFN-CERT-2022-0446
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-0036
dfn-cert: DFN-CERT-2021-0004
dfn-cert: DFN-CERT-2020-2807
dfn-cert: DFN-CERT-2020-2660
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-0820
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6244-1)

Summary
The remote host is missing an update for the 'amd64-microcode' package(s) announced via the USN-6244-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   amd64-microcode
Installed version:    amd64-microcode-3.20191218.1ubuntu1
Fixed version:      >=amd64-microcode-3.20191218.1ubuntu1.1
```

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

Affected Software/OS
'amd64-microcode' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Tavis Ormandy discovered that some AMD processors did not properly handle speculative execution of certain vector register instructions. A local attacker could use this to expose sensitive information.

... 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-6244-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6244.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6244-1
cve: CVE-2023-20593
advisory_id: USN-6244-1
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2902
cert-bund: WID-SEC-2023-1873
dfn-cert: DFN-CERT-2024-0246
dfn-cert: DFN-CERT-2023-3045
dfn-cert: DFN-CERT-2023-2984
dfn-cert: DFN-CERT-2023-2972
dfn-cert: DFN-CERT-2023-2916
dfn-cert: DFN-CERT-2023-2489
dfn-cert: DFN-CERT-2023-2342
dfn-cert: DFN-CERT-2023-2340
dfn-cert: DFN-CERT-2023-2274
dfn-cert: DFN-CERT-2023-2217
dfn-cert: DFN-CERT-2023-2213
dfn-cert: DFN-CERT-2023-2136
dfn-cert: DFN-CERT-2023-2112
dfn-cert: DFN-CERT-2023-2071
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-2037
dfn-cert: DFN-CERT-2023-2020
dfn-cert: DFN-CERT-2023-2017
dfn-cert: DFN-CERT-2023-2016
dfn-cert: DFN-CERT-2023-2009
dfn-cert: DFN-CERT-2023-2008
dfn-cert: DFN-CERT-2023-2007
dfn-cert: DFN-CERT-2023-2006
dfn-cert: DFN-CERT-2023-1968
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1953
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1898
dfn-cert: DFN-CERT-2023-1889

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1866
dfn-cert: DFN-CERT-2023-1849
dfn-cert: DFN-CERT-2023-1797
dfn-cert: DFN-CERT-2023-1789
dfn-cert: DFN-CERT-2023-1781
dfn-cert: DFN-CERT-2023-1767
dfn-cert: DFN-CERT-2023-1739
dfn-cert: DFN-CERT-2023-1733
dfn-cert: DFN-CERT-2023-1732
dfn-cert: DFN-CERT-2023-1682

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-6462-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6462-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.166.163
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Seth Jenkins discovered that the Linux kernel did not properly perform address randomization for a per-cpu memory management structure. A local attacker could use this to expose sensitive information (kernel memory) or in conjunction with another kernel vulnerability. (CVE-2023-0597)
Yu Hao and Weiteng Chen discovered that the Bluetooth HCI UART driver in the Linux kernel contained a race condition, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-31083)

... continues on next page ...

... continued from previous page ...

Lin Ma discovered that the Netlink Transformation (XFRM) subsystem in the Linux kernel contained a null pointer dereference vulnerability in some situations. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2023-3772)
It was discovered that the Siano USB MDTV receiver device driver in the Linux kernel did not properly handle device initialization failures in certain situations, leading to a use-after-free vulnerability. A physically proximate attacker could use this cause a denial of service (system crash). (CVE-2023-4132)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6462-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6462.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6462-1`
`cve: CVE-2023-0597`
`cve: CVE-2023-31083`
`cve: CVE-2023-3772`
`cve: CVE-2023-4132`
`advisory_id: USN-6462-1`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1957`
`cert-bund: WID-SEC-2023-1882`
`cert-bund: WID-SEC-2023-1062`
`cert-bund: WID-SEC-2023-0274`
`dfn-cert: DFN-CERT-2024-1398`
`dfn-cert: DFN-CERT-2024-1381`
`dfn-cert: DFN-CERT-2024-1165`
`dfn-cert: DFN-CERT-2024-0762`
`dfn-cert: DFN-CERT-2024-0730`
`dfn-cert: DFN-CERT-2024-0603`
`dfn-cert: DFN-CERT-2024-0513`
`dfn-cert: DFN-CERT-2024-0511`
`dfn-cert: DFN-CERT-2024-0333`
`dfn-cert: DFN-CERT-2024-0280`
`dfn-cert: DFN-CERT-2024-0249`
`dfn-cert: DFN-CERT-2024-0105`
`dfn-cert: DFN-CERT-2024-0094`
`dfn-cert: DFN-CERT-2023-3123`
`dfn-cert: DFN-CERT-2023-3121`
`dfn-cert: DFN-CERT-2023-2995`
`dfn-cert: DFN-CERT-2023-2994`
`dfn-cert: DFN-CERT-2023-2955`
`dfn-cert: DFN-CERT-2023-2888`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2779
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2686
dfn-cert: DFN-CERT-2023-2685
dfn-cert: DFN-CERT-2023-2684
dfn-cert: DFN-CERT-2023-2582
dfn-cert: DFN-CERT-2023-2580
dfn-cert: DFN-CERT-2023-2575
dfn-cert: DFN-CERT-2023-2574
dfn-cert: DFN-CERT-2023-2461
dfn-cert: DFN-CERT-2023-2406
dfn-cert: DFN-CERT-2023-2390
dfn-cert: DFN-CERT-2023-2389
dfn-cert: DFN-CERT-2023-2379
dfn-cert: DFN-CERT-2023-2219
dfn-cert: DFN-CERT-2023-2218
dfn-cert: DFN-CERT-2023-2214
dfn-cert: DFN-CERT-2023-2163
dfn-cert: DFN-CERT-2023-2162
dfn-cert: DFN-CERT-2023-2161
dfn-cert: DFN-CERT-2023-2103
dfn-cert: DFN-CERT-2023-2038
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1930
dfn-cert: DFN-CERT-2023-1923
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1647
dfn-cert: DFN-CERT-2023-1639
dfn-cert: DFN-CERT-2023-1577
dfn-cert: DFN-CERT-2023-1552
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-0728
dfn-cert: DFN-CERT-2023-0694
dfn-cert: DFN-CERT-2023-0693
dfn-cert: DFN-CERT-2023-0612
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-2023-0592
dfn-cert: DFN-CERT-2023-0586
dfn-cert: DFN-CERT-2023-0582
dfn-cert: DFN-CERT-2023-0262

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5493-1)

Summary
The remote host is missing an update for the 'linux, linux-hwe' package(s) announced via the USN-5493-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.121.122
```

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

Affected Software/OS
'linux, linux-hwe' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that the 8 Devices USB2CAN interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service (system crash).

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5493-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5493.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5493-1
cve: CVE-2022-28388
advisory_id: USN-5493-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2022-1319
cert-bund: WID-SEC-2022-0163
cert-bund: CB-K22/0437
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0745
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0105
dfn-cert: DFN-CERT-2023-2888
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2022-1962
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1677
dfn-cert: DFN-CERT-2022-1675
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1504
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1463
dfn-cert: DFN-CERT-2022-1423
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1278
dfn-cert: DFN-CERT-2022-1072
dfn-cert: DFN-CERT-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0862
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0860
dfn-cert: DFN-CERT-2022-0840
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0837
dfn-cert: DFN-CERT-2022-0819
dfn-cert: DFN-CERT-2022-0790
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5485-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-aws-5.13, linux-aws-hwe, linux-azure, linux-azure-4.15, linux-azure-5.4, linux-azure-5.13, linux-azure-fde, linux-dell300x, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gcp-5.13, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe, linux-hwe-5.4, linux-hwe-5.13, linux-ibm, linux-ibm-5.4, linux-intel-5.13, linux-intel-iotg, linux-kvm, linux-lowlatency, linux-oracle, linux-oracle-5.4, linux-oracle-5.13' package(s) announced via the USN-5485-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.120.121
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS

'linux, linux-aws, linux-aws-5.4, linux-aws-5.13, linux-aws-hwe, linux-azure, linux-azure-4.15, linux-azure-5.4, linux-azure-5.13, linux-azure-fde, linux-dell300x, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gcp-5.13, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe, linux-hwe-5.4, linux-hwe-5.13, linux-ibm, linux-ibm-5.4, linux-intel-5.13, linux-intel-iotg, linux-kvm, linux-lowlatency, linux-oracle, linux-oracle-5.4, linux-oracle-5.13' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight

It was discovered that some Intel processors did not completely perform cleanup actions on multi-core shared buffers. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21123)

It was discovered that some Intel processors did not completely perform cleanup actions on microarchitectural fill buffers. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21125)

It was discovered that some Intel processors did not properly perform cleanup during specific special register write operations. A local attacker could possibly use this to expose sensitive information. (CVE-2022-21166)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5485-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5485.1

Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5485-1
cve: CVE-2022-21123
cve: CVE-2022-21125
cve: CVE-2022-21166
advisory_id: USN-5485-1
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1432
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-2023-1230
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
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-1661
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1636
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1575
dfn-cert: DFN-CERT-2022-1552
dfn-cert: DFN-CERT-2022-1529
dfn-cert: DFN-CERT-2022-1523
dfn-cert: DFN-CERT-2022-1519
dfn-cert: DFN-CERT-2022-1488
dfn-cert: DFN-CERT-2022-1481
dfn-cert: DFN-CERT-2022-1424
dfn-cert: DFN-CERT-2022-1413
dfn-cert: DFN-CERT-2022-1405
dfn-cert: DFN-CERT-2022-1378
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1371
dfn-cert: DFN-CERT-2022-1369
dfn-cert: DFN-CERT-2022-1365
dfn-cert: DFN-CERT-2022-1358
dfn-cert: DFN-CERT-2022-1345
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1338
dfn-cert: DFN-CERT-2022-1336
dfn-cert: DFN-CERT-2022-1334
dfn-cert: DFN-CERT-2022-1333
dfn-cert: DFN-CERT-2022-1328
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5304-1)

Summary
The remote host is missing an update for the 'policykit-1' package(s) announced via the USN-5304-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   policykit-1
Installed version:    policykit-1-0.105-26ubuntu1.1
Fixed version:      >=policykit-1-0.105-26ubuntu1.3
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'policykit-1' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Kevin Backhouse discovered that PolicyKit incorrectly handled file descriptors. A local attacker could possibly use this issue to cause PolicyKit to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5304-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5304.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5304-1`
`cve: CVE-2021-4115`
`advisory_id: USN-5304-1`
`cert-bund: WID-SEC-2022-1335`
`cert-bund: WID-SEC-2022-1228`
`cert-bund: WID-SEC-2022-0773`
`cert-bund: CB-K22/0198`
`dfn-cert: DFN-CERT-2022-1143`
`dfn-cert: DFN-CERT-2022-0380`

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.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   systemd
Installed version:    systemd-245.4-4ubuntu3.7
Fixed version:      >=systemd-245.4-4ubuntu3.20
```

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

... continues on next page ...

... continued from previous page ...

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)
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: `2024-02-02T04:09:01Z`

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-2024-0794`
`cert-bund: WID-SEC-2023-1542`
`cert-bund: WID-SEC-2023-1021`
`cert-bund: WID-SEC-2022-2384`
`cert-bund: WID-SEC-2022-2165`
`cert-bund: WID-SEC-2022-2012`
`dfn-cert: DFN-CERT-2023-1590`
`dfn-cert: DFN-CERT-2023-0764`
`dfn-cert: DFN-CERT-2022-2924`
`dfn-cert: DFN-CERT-2022-2897`
`dfn-cert: DFN-CERT-2022-2481`

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5384-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) announced via the USN-5384-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.109.113
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-azure-fde, linux-gcp, linux-gcp-5.4, linux-gke, linux-gke-5.4, linux-gkeop, linux-gkeop-5.4, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that the UDF file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious UDF image that, when mounted and operated on, could cause a denial of service (system crash). (CVE-2022-0617)
Lyu Tao discovered that the NFS implementation in the Linux kernel did not properly handle requests to open a directory on a regular file. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2022-24448)
It was discovered that the YAM AX.25 device driver in the Linux kernel did not properly deallocate memory in some error conditions. A local privileged attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2022-24959)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5384-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5384.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5384-1
cve: CVE-2022-0617
cve: CVE-2022-24448
cve: CVE-2022-24959
advisory_id: USN-5384-1
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1969
cert-bund: WID-SEC-2022-0793
cert-bund: WID-SEC-2022-0319
cert-bund: WID-SEC-2022-0149
cert-bund: CB-K22/0296
cert-bund: CB-K22/0177
cert-bund: CB-K22/0141
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2023-0866
dfn-cert: DFN-CERT-2023-0861
dfn-cert: DFN-CERT-2023-0606
dfn-cert: DFN-CERT-2022-2569
dfn-cert: DFN-CERT-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-1640
dfn-cert: DFN-CERT-2022-1343
dfn-cert: DFN-CERT-2022-1342
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0901
dfn-cert: DFN-CERT-2022-0896
dfn-cert: DFN-CERT-2022-0895
dfn-cert: DFN-CERT-2022-0861
dfn-cert: DFN-CERT-2022-0803
dfn-cert: DFN-CERT-2022-0721
dfn-cert: DFN-CERT-2022-0720
dfn-cert: DFN-CERT-2022-0719
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0550
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
dfn-cert: DFN-CERT-2022-0545
dfn-cert: DFN-CERT-2022-0544
dfn-cert: DFN-CERT-2022-0542
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0540
dfn-cert: DFN-CERT-2022-0538
dfn-cert: DFN-CERT-2022-0537
dfn-cert: DFN-CERT-2022-0513
dfn-cert: DFN-CERT-2022-0439
dfn-cert: DFN-CERT-2022-0433

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5786-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'nautilus' package(s) announced via the USN-5786-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   nautilus
Installed version:    nautilus-1:3.36.3-0ubuntu1
Fixed version:      >=nautilus-1:3.36.3-0ubuntu1.20.04.2
```

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

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

Vulnerability Insight
It was discovered that GNOME Files incorrectly handled certain filenames. An attacker could possibly use this issue to cause GNOME Files to crash, leading to a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5786-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5786.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5786-1
cve: CVE-2022-37290
advisory_id: USN-5786-1
cert-bund: WID-SEC-2023-2031
dfn-cert: DFN-CERT-2023-1643
dfn-cert: DFN-CERT-2022-2803
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5077-1)

Summary
The remote host is missing an update for the 'apport' package(s) announced via the USN-5077-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   apport
Installed version:    apport-2.20.11-0ubuntu27.18
Fixed version:      >=apport-2.20.11-0ubuntu27.20
Vulnerable package:   python3-apport
Installed version:    python3-apport-2.20.11-0ubuntu27.18
Fixed version:      >=python3-apport-2.20.11-0ubuntu27.20
```

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

Affected Software/OS
'apport' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Maik Munch and Stephen Rottger discovered that Apport incorrectly handled certain information gathering operations. A local attacker could use this issue to gain read access to arbitrary files, possibly containing sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5077-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5077.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5077-1
cve: CVE-2021-3709
cve: CVE-2021-3710
advisory_id: USN-5077-1
dfn-cert: DFN-CERT-2021-1923
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5898-1)

Summary
The remote host is missing an update for the 'openjdk-8' package(s) announced via the USN-5898-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u362-ga-0ubuntu1~20.04.1
```

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u362-ga-0ubuntu1~20.04.1
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u362-ga-0ubuntu1~20.04.1
```

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

Affected Software/OS
'openjdk-8' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that the Serialization component of OpenJDK did not properly handle the deserialization of some CORBA objects. An attacker could possibly use this to bypass Java sandbox restrictions. (CVE-2023-21830)
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-5898-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5898.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5898-1
cve: CVE-2023-21830
cve: CVE-2023-21843
advisory_id: USN-5898-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-2164
cert-bund: WID-SEC-2023-1813
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0840
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0128
dfn-cert: DFN-CERT-2023-1425
dfn-cert: DFN-CERT-2023-1174
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1139
dfn-cert: DFN-CERT-2023-0846
dfn-cert: DFN-CERT-2023-0717
dfn-cert: DFN-CERT-2023-0605
dfn-cert: DFN-CERT-2023-0372
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: 5.3)
NVT: Ubuntu: Security Advisory (USN-6528-1)

Summary
The remote host is missing an update for the 'openjdk-8' package(s) announced via the USN-6528-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u392-ga-1~20.04
Vulnerable package:   openjdk-8-jdk-headless
Installed version:    openjdk-8-jdk-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-headless-8u392-ga-1~20.04
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u392-ga-1~20.04
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u392-ga-1~20.04
```

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

Affected Software/OS
'openjdk-8' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that the HotSpot VM implementation in OpenJDK did not properly validate bytecode blocks in certain situations. An attacker could possibly use this to cause a denial of service. (CVE-2022-40433)

... continues on next page ...

... continued from previous page ...

Carter Kozak discovered that OpenJDK, when compiling with AVX-512 instruction support enabled, could produce code that resulted in memory corruption in certain situations. An attacker targeting applications built in this way could possibly use this to cause a denial of service or execute arbitrary code. In Ubuntu, OpenJDK defaults to not using AVX-512 instructions. (CVE-2023-22025)
It was discovered that the CORBA implementation in OpenJDK did not properly perform deserialization of IOR string objects. An attacker could possibly use this to bypass Java sandbox restrictions. (CVE-2023-22067)
It was discovered that OpenJDK did not properly perform PKIX certification path validation in certain situations. An attacker could use this to cause a denial of service. (CVE-2023-22081)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6528-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6528.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6528-1`
`cve: CVE-2022-40433`
`cve: CVE-2023-22025`
`cve: CVE-2023-22067`
`cve: CVE-2023-22081`
`advisory_id: USN-6528-1`
`cert-bund: WID-SEC-2024-0769`
`cert-bund: WID-SEC-2024-0528`
`cert-bund: WID-SEC-2024-0521`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-2692`
`cert-bund: WID-SEC-2023-2235`
`dfn-cert: DFN-CERT-2024-0169`
`dfn-cert: DFN-CERT-2023-3177`
`dfn-cert: DFN-CERT-2023-3009`
`dfn-cert: DFN-CERT-2023-3006`
`dfn-cert: DFN-CERT-2023-2999`
`dfn-cert: DFN-CERT-2023-2975`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-2939`
`dfn-cert: DFN-CERT-2023-2886`
`dfn-cert: DFN-CERT-2023-2562`
`dfn-cert: DFN-CERT-2023-2561`
`dfn-cert: DFN-CERT-2023-2560`
`dfn-cert: DFN-CERT-2023-2559`
`dfn-cert: DFN-CERT-2023-2558`
`dfn-cert: DFN-CERT-2023-2557`
`dfn-cert: DFN-CERT-2023-2535`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2534

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5007-1)

Summary
The remote host is missing an update for the 'libuv1' package(s) announced via the USN-5007-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libuv1
Installed version: libuv1-1.34.2-1ubuntu1.1
Fixed version: >=libuv1-1.34.2-1ubuntu1.3

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

Affected Software/OS
'libuv1' package(s) on Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04.

Vulnerability Insight
Eric Sesterhenn discovered that libuv incorrectly handled certain strings. An attacker could possibly use this issue to access 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-5007-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5007.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5007-1
cve: CVE-2021-22918
advisory_id: USN-5007-1
cert-bund: WID-SEC-2024-0042
cert-bund: WID-SEC-2023-0856
cert-bund: CB-K21/0714
dfn-cert: DFN-CERT-2021-1988
dfn-cert: DFN-CERT-2021-1862
dfn-cert: DFN-CERT-2021-1620
dfn-cert: DFN-CERT-2021-1500
dfn-cert: DFN-CERT-2021-1447

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2021-1433

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-6513-2)

Summary
The remote host is missing an update for the 'python3.8, python3.10, python3.11' package(s) announced via the USN-6513-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3.8
Installed version: python3.8-3.8.5-1~20.04.3
Fixed version: >=python3.8-3.8.10-0ubuntu1~20.04.9

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

Affected Software/OS
'python3.8, python3.10, python3.11' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
USN-6513-1 fixed vulnerabilities in Python. This update provides the corresponding updates for Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 23.04.
Original advisory details:
It was discovered that Python incorrectly handled certain plist files. If a user or an automated system were tricked into processing a specially crafted plist file, an attacker could possibly use this issue to consume resources, resulting in a denial of service. (CVE-2022-48564)
It was discovered that Python instances of ssl.SSLSocket were vulnerable to a bypass of the TLS handshake. An attacker could possibly use this issue to cause applications to treat unauthenticated received data before TLS handshake as authenticated data after TLS handshake. (CVE-2023-40217)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6513-2)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6513.2
Version used: 2024-02-28T10:02:42Z

References
url: https://ubuntu.com/security/notices/USN-6513-2
cve: CVE-2023-40217
advisory_id: USN-6513-2

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2850
cert-bund: WID-SEC-2023-2173
dfn-cert: DFN-CERT-2024-0610
dfn-cert: DFN-CERT-2024-0609
dfn-cert: DFN-CERT-2023-3168
dfn-cert: DFN-CERT-2023-2954
dfn-cert: DFN-CERT-2023-2941
dfn-cert: DFN-CERT-2023-2783
dfn-cert: DFN-CERT-2023-2768
dfn-cert: DFN-CERT-2023-2714
dfn-cert: DFN-CERT-2023-2485
dfn-cert: DFN-CERT-2023-2370
dfn-cert: DFN-CERT-2023-2227
dfn-cert: DFN-CERT-2023-2226
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-6435-2)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-6435-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libssl1.1
Installed version:    libssl1.1-1.1.1f-1ubuntu2.4
Fixed version:      >=libssl1.1-1.1.1f-1ubuntu2.20
Vulnerable package:   openssl
Installed version:    openssl-1.1.1f-1ubuntu2.4
Fixed version:      >=openssl-1.1.1f-1ubuntu2.20
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6435-1 fixed vulnerabilities in OpenSSL. This update provides the corresponding updates for Ubuntu 20.04 LTS.
Original advisory details:

... continues on next page ...

... continued from previous page ...

It was discovered that OpenSSL incorrectly handled excessively large Diffie-Hellman parameters. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3446)
Bernd Edlinger discovered that OpenSSL incorrectly handled excessively large Diffie-Hellman parameters. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3817)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6435-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6435.2
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6435-2`
`cve: CVE-2023-3446`
`cve: CVE-2023-3817`
`advisory_id: USN-6435-2`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2024-1226`
`cert-bund: WID-SEC-2024-0123`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2024-0053`
`cert-bund: WID-SEC-2023-2964`
`cert-bund: WID-SEC-2023-2690`
`cert-bund: WID-SEC-2023-1926`
`cert-bund: WID-SEC-2023-1833`
`dfn-cert: DFN-CERT-2024-1166`
`dfn-cert: DFN-CERT-2024-1157`
`dfn-cert: DFN-CERT-2024-1067`
`dfn-cert: DFN-CERT-2024-0764`
`dfn-cert: DFN-CERT-2024-0746`
`dfn-cert: DFN-CERT-2024-0224`
`dfn-cert: DFN-CERT-2024-0191`
`dfn-cert: DFN-CERT-2024-0147`
`dfn-cert: DFN-CERT-2024-0133`
`dfn-cert: DFN-CERT-2023-3071`
`dfn-cert: DFN-CERT-2023-3070`
`dfn-cert: DFN-CERT-2023-2960`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-2643`
`dfn-cert: DFN-CERT-2023-2624`
`dfn-cert: DFN-CERT-2023-2615`
`dfn-cert: DFN-CERT-2023-2536`
`dfn-cert: DFN-CERT-2023-2116`
`dfn-cert: DFN-CERT-2023-1897`
`dfn-cert: DFN-CERT-2023-1856`
`dfn-cert: DFN-CERT-2023-1769`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1760
dfn-cert: DFN-CERT-2023-1748
dfn-cert: DFN-CERT-2023-1738
dfn-cert: DFN-CERT-2023-1661

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5502-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5502-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssl1.1
Installed version: libssl1.1-1.1.1f-1ubuntu2.4
Fixed version: >=libssl1.1-1.1.1f-1ubuntu2.16

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

Affected Software/OS
'openssl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
Alex Chernyakhovsky discovered that OpenSSL incorrectly handled AES OCB mode when using the AES-NI assembly optimized implementation on 32-bit x86 platforms. A remote 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-5502-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5502.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-5502-1
cve: CVE-2022-2097
advisory_id: USN-5502-1
cert-bund: WID-SEC-2024-1186
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-1969

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1777
cert-bund: WID-SEC-2022-1776
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1245
cert-bund: WID-SEC-2022-1146
cert-bund: WID-SEC-2022-1068
cert-bund: WID-SEC-2022-1065
cert-bund: WID-SEC-2022-0561
dfn-cert: DFN-CERT-2024-0147
dfn-cert: DFN-CERT-2023-2667
dfn-cert: DFN-CERT-2023-2491
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0299
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2022-2315
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2150
dfn-cert: DFN-CERT-2022-2073
dfn-cert: DFN-CERT-2022-2072
dfn-cert: DFN-CERT-2022-1905
dfn-cert: DFN-CERT-2022-1646
dfn-cert: DFN-CERT-2022-1536
dfn-cert: DFN-CERT-2022-1521
dfn-cert: DFN-CERT-2022-1520
dfn-cert: DFN-CERT-2022-1515
dfn-cert: DFN-CERT-2022-1497

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-6592-1)

Summary
The remote host is missing an update for the 'libssh' package(s) announced via the USN-6592-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libssh-4
Installed version: libssh-4-0.9.3-2ubuntu2.1
Fixed version: >=libssh-4-0.9.3-2ubuntu2.5

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'libssh' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that libssh incorrectly handled the ProxyCommand and the ProxyJump features. A remote attacker could possibly use this issue to inject malicious code into the command of the features mentioned through the hostname parameter. (CVE-2023-6004)
It was discovered that libssh incorrectly handled return codes when performing message digest operations. A remote attacker could possibly use this issue to cause libssh to crash, obtain sensitive information, or execute arbitrary code. (CVE-2023-6918)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6592-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6592.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6592-1`
`cve: CVE-2023-6004`
`cve: CVE-2023-6918`
`advisory_id: USN-6592-1`
`cert-bund: WID-SEC-2024-1307`
`cert-bund: WID-SEC-2023-3175`
`dfn-cert: DFN-CERT-2024-0440`
`dfn-cert: DFN-CERT-2024-0285`
`dfn-cert: DFN-CERT-2024-0171`
`dfn-cert: DFN-CERT-2024-0154`
`dfn-cert: DFN-CERT-2023-3184`

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5021-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5021-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.6
Vulnerable package:   libcurl3-gnutls
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.6
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.6
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Harry Sintonen and Tomas Hoger discovered that curl incorrectly handled TELNET connections when the -t option was used on the command line. Uninitialized data possibly containing sensitive information could be sent to the remote server, contrary to expectations. (CVE-2021-22898, CVE-2021-22925)
Harry Sintonen discovered that curl incorrectly reused connections in the connection pool. This could result in curl reusing the wrong connections. (CVE-2021-22924)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5021-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5021.1
Version used: `2024-02-02T04:09:01Z`

References

```
url: https://ubuntu.com/security/notices/USN-5021-1
cve: CVE-2021-22898
cve: CVE-2021-22924
cve: CVE-2021-22925
advisory_id: USN-5021-1
cert-bund: WID-SEC-2024-0556
cert-bund: WID-SEC-2023-2229
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1225
cert-bund: WID-SEC-2022-0874
cert-bund: WID-SEC-2022-0873
cert-bund: CB-K22/0044
cert-bund: CB-K21/0994
cert-bund: CB-K21/0797
dfn-cert: DFN-CERT-2024-0573
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
dfn-cert: DFN-CERT-2022-0835
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2022-0112
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2369
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
dfn-cert: DFN-CERT-2021-2189
dfn-cert: DFN-CERT-2021-2167
dfn-cert: DFN-CERT-2021-1917
dfn-cert: DFN-CERT-2021-1915
dfn-cert: DFN-CERT-2021-1743
dfn-cert: DFN-CERT-2021-1593
dfn-cert: DFN-CERT-2021-1580
dfn-cert: DFN-CERT-2021-1568
dfn-cert: DFN-CERT-2021-1174
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-1157
dfn-cert: DFN-CERT-2021-1151
dfn-cert: DFN-CERT-2021-1148
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-6005-1)

Summary
The remote host is missing an update for the 'sudo' package(s) announced via the USN-6005-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:    sudo
Installed version:     sudo-1.8.31-1ubuntu1.2
Fixed version:      >=sudo-1.8.31-1ubuntu1.5
```

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

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

Vulnerability Insight
Matthieu Barjole and Victor Cutillas discovered that Sudo incorrectly escaped control characters in log messages and sudoreplay output. An attacker could possibly use these issues to inject terminal control characters that alter output when being viewed.

... 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-6005-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6005.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6005-1
cve: CVE-2023-28486
cve: CVE-2023-28487
advisory_id: USN-6005-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-2031
cert-bund: WID-SEC-2023-0667
dfn-cert: DFN-CERT-2024-0762
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0395
dfn-cert: DFN-CERT-2024-0303
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-1196
dfn-cert: DFN-CERT-2023-0704
dfn-cert: DFN-CERT-2023-0702

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5313-2)

Summary
The remote host is missing an update for the 'openjdk-lts' package(s) announced via the USN-5313-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: openjdk-11-jre
Installed version: openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-11.0.14.1+1-0ubuntu1~20.04
Vulnerable package: openjdk-11-jre-headless
Installed version: openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-headless-11.0.14.1+1-0ubuntu1~20.04

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
USN-5313-1 fixed vulnerabilities and added features in OpenJDK. Unfortunately, that update introduced a regression in OpenJDK 11 that could impact interoperability with some popular HTTP/2 servers making it unable to connect to said servers. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that OpenJDK incorrectly handled deserialization filters. An attacker could possibly use this issue to insert, delete or obtain sensitive information. (CVE-2022-21248)
It was discovered that OpenJDK incorrectly read uncompressed TIFF files. An attacker could possibly use this issue to cause a denial of service via a specially crafted TIFF file. (CVE-2022-21277)
Jonni Passki discovered that OpenJDK incorrectly verified access restrictions when performing URI resolution. An attacker could possibly use this issue to obtain sensitive information. (CVE-2022-21282)
It was discovered that OpenJDK incorrectly handled certain regular expressions in the Pattern class implementation. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21283)
It was discovered that OpenJDK incorrectly handled specially crafted Java class files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21291)
Markus Loewe discovered that OpenJDK incorrectly validated attributes during object deserialization. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21293, CVE-2022-21294)
Dan Rabe discovered that OpenJDK incorrectly verified access permissions in the JAXP component. An attacker could possibly use this to specially craft an XML file to obtain sensitive information. (CVE-2022-21296)
It was discovered that OpenJDK incorrectly handled XML entities. An attacker could use this to specially craft an XML file that, when parsed, would possibly cause a denial of service. (CVE-2022-21299)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array indexes. An attacker could possibly use this issue to obtain sensitive information. (CVE-2022-21305)
It was discovered that OpenJDK incorrectly read very long attributes values in JAR file manifests. An attacker could possibly use this to specially craft JAR file to cause a denial of service. (CVE-2022-21340)
It was discovered that OpenJDK incorrectly validated input from serialized streams. An attacker cold possibly use this issue to bypass sandbox restrictions. (CVE-2022-21341)
Fabian Meumertzheim discovered that OpenJDK incorrectly handled certain specially crafted BMP or TIFF files. An attacker could possibly use this to cause a denial of service. (CVE-2022-21360, CVE-2022-21366)
It was discovered that an integer overflow could be triggered in OpenJDK BMPImageReader class implementation. An attacker could possibly use this to specially craft a BMP file to cause a denial of service. (CVE-2022-21365)

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-5313-2)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5313.2
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5313-2
url: https://launchpad.net/bugs/1966338
cve: CVE-2022-21248
cve: CVE-2022-21277
cve: CVE-2022-21282
cve: CVE-2022-21283
cve: CVE-2022-21291
cve: CVE-2022-21293
cve: CVE-2022-21294
cve: CVE-2022-21296
cve: CVE-2022-21299
cve: CVE-2022-21305
cve: CVE-2022-21340
cve: CVE-2022-21341
cve: CVE-2022-21360
cve: CVE-2022-21365
cve: CVE-2022-21366
advisory_id: USN-5313-2
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0100
cert-bund: WID-SEC-2022-0028

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1266
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0111

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5313-1)

Summary
The remote host is missing an update for the 'openjdk-17, openjdk-lts' package(s) announced via the USN-5313-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.14+9-0ubuntu2~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.14+9-0ubuntu2~20.04
```

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

Affected Software/OS
'openjdk-17, openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that OpenJDK incorrectly handled deserialization filters. An attacker could possibly use this issue to insert, delete or obtain sensitive information. (CVE-2022-21248)
It was discovered that OpenJDK incorrectly read uncompressed TIFF files. An attacker could possibly use this issue to cause a denial of service via a specially crafted TIFF file. (CVE-2022-21277)
Jonni Passki discovered that OpenJDK incorrectly verified access restrictions when performing URI resolution. An attacker could possibly use this issue to obtain sensitive information. (CVE-2022-21282)

... continues on next page ...

... continued from previous page ...

It was discovered that OpenJDK incorrectly handled certain regular expressions in the Pattern class implementation. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21283)
It was discovered that OpenJDK incorrectly handled specially crafted Java class files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21291)
Markus Loewe discovered that OpenJDK incorrectly validated attributes during object deserialization. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21293, CVE-2022-21294)
Dan Rabe discovered that OpenJDK incorrectly verified access permissions in the JAXP component. An attacker could possibly use this to specially craft an XML file to obtain sensitive information. (CVE-2022-21296)
It was discovered that OpenJDK incorrectly handled XML entities. An attacker could use this to specially craft an XML file that, when parsed, would possibly cause a denial of service. (CVE-2022-21299)
Zhiqiang Zang discovered that OpenJDK incorrectly handled array indexes. An attacker could possibly use this issue to obtain sensitive information. (CVE-2022-21305)
It was discovered that OpenJDK incorrectly read very long attributes values in JAR file manifests. An attacker could possibly use this to specially craft JAR file to cause a denial of service. (CVE-2022-21340)
It was discovered that OpenJDK incorrectly validated input from serialized streams. An attacker cold possibly use this issue to bypass sandbox restrictions. (CVE-2022-21341)
Fabian Meumertzheim discovered that OpenJDK incorrectly handled certain specially crafted BMP or TIFF files. An attacker could possibly use this to cause a denial of service. (CVE-2022-21360, CVE-2022-21366)
It was discovered that an integer overflow could be triggered in OpenJDK BMPImageReader class implementation. An attacker could possibly use this to specially craft a BMP file to cause a denial of service. (CVE-2022-21365)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5313-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5313.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5313-1`
`cve: CVE-2022-21248`
`cve: CVE-2022-21277`
`cve: CVE-2022-21282`
`cve: CVE-2022-21283`
`cve: CVE-2022-21291`
`cve: CVE-2022-21293`
`cve: CVE-2022-21294`
`cve: CVE-2022-21296`
`cve: CVE-2022-21299`
`cve: CVE-2022-21305`
`cve: CVE-2022-21340`

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-21341
cve: CVE-2022-21360
cve: CVE-2022-21365
cve: CVE-2022-21366
advisory_id: USN-5313-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0839
cert-bund: WID-SEC-2023-0838
cert-bund: WID-SEC-2022-1335
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0987
cert-bund: WID-SEC-2022-0858
cert-bund: WID-SEC-2022-0833
cert-bund: WID-SEC-2022-0826
cert-bund: WID-SEC-2022-0812
cert-bund: WID-SEC-2022-0799
cert-bund: WID-SEC-2022-0745
cert-bund: WID-SEC-2022-0712
cert-bund: WID-SEC-2022-0472
cert-bund: WID-SEC-2022-0447
cert-bund: WID-SEC-2022-0446
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0431
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0300
cert-bund: WID-SEC-2022-0287
cert-bund: WID-SEC-2022-0203
cert-bund: WID-SEC-2022-0100
cert-bund: WID-SEC-2022-0028
cert-bund: CB-K22/0078
dfn-cert: DFN-CERT-2022-1648
dfn-cert: DFN-CERT-2022-1339
dfn-cert: DFN-CERT-2022-1323
dfn-cert: DFN-CERT-2022-1266
dfn-cert: DFN-CERT-2022-0451
dfn-cert: DFN-CERT-2022-0438
dfn-cert: DFN-CERT-2022-0320
dfn-cert: DFN-CERT-2022-0111

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-5719-1)

Summary
The remote host is missing an update for the 'openjdk-8, openjdk-17, openjdk-19, openjdk-lts' package(s) announced via the USN-5719-1 advisory.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.17+8-1ubuntu2~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.17+8-1ubuntu2~20.04
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u352-ga-1~20.04
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u352-ga-1~20.04
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u352-ga-1~20.04
```

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

Affected Software/OS
'openjdk-8, openjdk-17, openjdk-19, openjdk-lts' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

Vulnerability Insight
It was discovered that OpenJDK incorrectly handled long client hostnames. An attacker could possibly use this issue to cause the corruption of sensitive information. (CVE-2022-21619)
It was discovered that OpenJDK incorrectly randomized DNS port numbers. A remote attacker could possibly use this issue to perform spoofing attacks. (CVE-2022-21624)
It was discovered that OpenJDK did not limit the number of connections accepted from HTTP clients. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-21628)
It was discovered that OpenJDK incorrectly handled X.509 certificates. An attacker could possibly use this issue to cause a denial of service. This issue only affected OpenJDK 8 and OpenJDK 11. (CVE-2022-21626)
It was discovered that OpenJDK incorrectly handled cached server connections. An attacker could possibly use this issue to perform spoofing attacks. This issue only affected OpenJDK 11, OpenJDK 17 and OpenJDK 19. (CVE-2022-39399)
It was discovered that OpenJDK incorrectly handled byte conversions. An attacker could possibly use this issue to obtain sensitive information. This issue only affected OpenJDK 11, OpenJDK 17 and OpenJDK 19. (CVE-2022-21618)

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-5719-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5719.1
Version used: 2024-02-02T04:09:01Z

References

url: https://ubuntu.com/security/notices/USN-5719-1
cve: CVE-2022-21618
cve: CVE-2022-21619
cve: CVE-2022-21624
cve: CVE-2022-21626
cve: CVE-2022-21628
cve: CVE-2022-39399
advisory_id: USN-5719-1
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2023-0809
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1789
dfn-cert: DFN-CERT-2023-0616
dfn-cert: DFN-CERT-2023-0608
dfn-cert: DFN-CERT-2023-0607
dfn-cert: DFN-CERT-2023-0256
dfn-cert: DFN-CERT-2023-0217
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-2696
dfn-cert: DFN-CERT-2022-2660
dfn-cert: DFN-CERT-2022-2600
dfn-cert: DFN-CERT-2022-2547
dfn-cert: DFN-CERT-2022-2313
dfn-cert: DFN-CERT-2022-2312

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.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: openjdk-11-jre
Installed version: openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-11.0.18+10-0ubuntu1~20.04.1
Vulnerable package: openjdk-11-jre-headless
Installed version: openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version: >=openjdk-11-jre-headless-11.0.18+10-0ubuntu1~20.04.1

... continues on next page ...

... continued from previous page ...

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

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: `2024-02-02T04:09:01Z`

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-2024-0794`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2625`
`cert-bund: WID-SEC-2023-2164`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-0561`
`cert-bund: WID-SEC-2023-0128`
`dfn-cert: DFN-CERT-2023-1174`
`dfn-cert: DFN-CERT-2023-1139`
`dfn-cert: DFN-CERT-2023-0846`
`dfn-cert: DFN-CERT-2023-0717`
`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: 5.3)
NVT: Ubuntu: Security Advisory (USN-6527-1)

Summary
The remote host is missing an update for the 'openjdk-17, openjdk-21, openjdk-lts' package(s) announced via the USN-6527-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.21+9-0ubuntu1~20.04
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.21+9-0ubuntu1~20.04
```

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

Affected Software/OS
'openjdk-17, openjdk-21, openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Carter Kozak discovered that OpenJDK, when compiling with AVX-512 instruction support enabled, could produce code that resulted in memory corruption in certain situations. An attacker targeting applications built in this way could possibly use this to cause a denial of service or execute arbitrary code. In Ubuntu, OpenJDK defaults to not using AVX-512 instructions. (CVE-2023-22025)
It was discovered that OpenJDK did not properly perform PKIX certification path validation in certain situations. An attacker could use this to cause a denial of service. (CVE-2023-22081)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6527-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6527.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6527-1
cve: CVE-2023-22025
cve: CVE-2023-22081
advisory_id: USN-6527-1
cert-bund: WID-SEC-2024-0769
cert-bund: WID-SEC-2024-0528
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2024-0521
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2692
dfn-cert: DFN-CERT-2024-0169
dfn-cert: DFN-CERT-2023-3177
dfn-cert: DFN-CERT-2023-3009
dfn-cert: DFN-CERT-2023-3006
dfn-cert: DFN-CERT-2023-2999
dfn-cert: DFN-CERT-2023-2975
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2023-2886
dfn-cert: DFN-CERT-2023-2562
dfn-cert: DFN-CERT-2023-2561
dfn-cert: DFN-CERT-2023-2560
dfn-cert: DFN-CERT-2023-2559
dfn-cert: DFN-CERT-2023-2558
dfn-cert: DFN-CERT-2023-2557
dfn-cert: DFN-CERT-2023-2535
dfn-cert: DFN-CERT-2023-2534

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5037-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-5037-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-91.0.2+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
USN-5037-1 fixed vulnerabilities in Firefox. The update introduced a regression that caused Firefox to repeatedly prompt for a password. This update fixes the problem.

... continues on next page ...

... continued from previous page ...

We apologize for the inconvenience.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5037-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5037.2
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5037-2`
`url: https://launchpad.net/bugs/1941496`
`advisory_id: USN-5037-2`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6721-2)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6721-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.17
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.17
```

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

Affected Software/OS
'xorg-server, xwayland' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

USN-6721-1 fixed vulnerabilities in X.Org X Server. That fix was incomplete resulting in a regression. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that X.Org X Server incorrectly handled certain data. An attacker could possibly use this issue to expose sensitive information. (CVE-2024-31080, CVE-2024-31081, CVE-2024-31082)
It was discovered that X.Org X Server incorrectly handled certain glyphs. An attacker could possibly use this issue to cause a crash or expose sensitive information. (CVE-2024-31083)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6721-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6721.2
Version used: `2024-04-10T04:08:49Z`

References
`url: https://ubuntu.com/security/notices/USN-6721-2`
`url: https://launchpad.net/bugs/2060354`
`cve: CVE-2024-31080`
`cve: CVE-2024-31081`
`cve: CVE-2024-31082`
`cve: CVE-2024-31083`
`advisory_id: USN-6721-2`
`cert-bund: WID-SEC-2024-0778`
`dfn-cert: DFN-CERT-2024-0982`
`dfn-cert: DFN-CERT-2024-0976`
`dfn-cert: DFN-CERT-2024-0877`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5122-1)

Summary
The remote host is missing an update for the 'apport' package(s) announced via the USN-5122-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   apport
Installed version:    apport-2.20.11-0ubuntu27.18
Fixed version:      >=apport-2.20.11-0ubuntu27.21
Vulnerable package:   python3-apport
Installed version:    python3-apport-2.20.11-0ubuntu27.18
Fixed version:      >=python3-apport-2.20.11-0ubuntu27.21
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'apport' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04, Ubuntu 21.10.

Vulnerability Insight
It was discovered that Apport could be tricked into writing core files as root into arbitrary directories in certain scenarios. A local attacker could possibly use this issue to escalate privileges. This update will cause Apport to generate all core files in the /var/lib/apport/coredump directory.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5122-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5122.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5122-1`
`url: https://launchpad.net/bugs/1948657`
`advisory_id: USN-5122-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6830-1)

Summary
The remote host is missing an update for the 'libndp' package(s) announced via the USN-6830-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libndp0
Installed version:    libndp0-1.7-0ubuntu1
Fixed version:      >=libndp0-1.7-0ubuntu1.1
```

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

Affected Software/OS
'libndp' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that libndp incorrectly handled certain malformed IPv6 router advertisement packets. A local attacker could use this issue to cause NetworkManager to crash, resulting in 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-6830-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6830.1
Version used: `2024-06-13T04:07:56Z`

References
`url: https://ubuntu.com/security/notices/USN-6830-1`
`cve: CVE-2024-5564`
`advisory_id: USN-6830-1`
`dfn-cert: DFN-CERT-2024-1551`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5481-1)

Summary
The remote host is missing an update for the 'bluez' package(s) announced via the USN-5481-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   bluez
Installed version:    bluez-5.53-0ubuntu3.2
Fixed version:      >=bluez-5.53-0ubuntu3.6
Vulnerable package:   libbluetooth3
Installed version:    libbluetooth3-5.53-0ubuntu3.2
Fixed version:      >=libbluetooth3-5.53-0ubuntu3.6
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was discovered that BlueZ incorrectly validated certain capabilities and lengths when handling the A2DP profile. A remote attacker could use this issue to cause BlueZ to crash, resulting in 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-5481-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5481.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5481-1`
`url: https://launchpad.net/bugs/1977968`
`advisory_id: USN-5481-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5086-1)

Summary
The remote host is missing an update for the 'linux, linux-hwe, linux-hwe-5.4, linux-hwe-5.11' package(s) announced via the USN-5086-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.86.90
```

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

Affected Software/OS
'linux, linux-hwe, linux-hwe-5.4, linux-hwe-5.11' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
Johan Almbladh discovered that the eBPF JIT implementation for IBM s390x systems in the Linux kernel miscompiled operations in some situations, allowing circumvention of the BPF verifier. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

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-5086-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5086.1
Version used: 2022-09-13T14:14:11Z

References
url: https://ubuntu.com/security/notices/USN-5086-1
url: https://launchpad.net/bugs/1943960
advisory_id: USN-5086-1

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6797-1)

Summary
The remote host is missing an update for the 'intel-microcode' package(s) announced via the USN-6797-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: intel-microcode
Installed version: intel-microcode-3.20210608.0ubuntu0.20.04.1
Fixed version: >=intel-microcode-3.20240514.0ubuntu0.20.04.1

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 23.10, Ubuntu 24.04.

Vulnerability Insight
It was discovered that some 3rd and 4th Generation Intel(r) Xeon(r) Processors did not properly restrict access to certain hardware features when using Intel(r) SGX or Intel(r) TDX. This may allow a privileged local user to potentially further escalate their privileges on the system. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-22655)
It was discovered that some Intel(r) Atom(r) Processors did not properly clear register state when performing various operations. A local attacker could use this to obtain sensitive information via a transient execution attack. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-28746)
It was discovered that some Intel(r) Processors did not properly clear the state of various hardware structures when switching execution contexts. A local attacker could use this to access privileged information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-38575)

... continues on next page ...

... continued from previous page ...

It was discovered that some Intel(r) Processors did not properly enforce bus lock regulator protections. A remote attacker could use this to cause a denial of service. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-39368)
It was discovered that some Intel(r) Xeon(r) D Processors did not properly calculate the SGX base key when using Intel(r) SGX. A privileged local attacker could use this to obtain sensitive information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-43490)
It was discovered that some Intel(r) Processors did not properly protect against concurrent accesses. A local attacker could use this to obtain sensitive information. (CVE-2023-45733)
It was discovered that some Intel(r) Processors TDX module software did not properly validate input. A privileged local attacker could use this information to potentially further escalate their privileges on the system. (CVE-2023-45745, CVE-2023-47855)
It was discovered that some Intel(r) Core(tm) Ultra processors did not properly handle particular instruction sequences. A local attacker could use this issue to cause a denial of service. (CVE-2023-46103)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6797-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6797.1
Version used: `2024-05-30T04:08:53Z`

References
`url: https://ubuntu.com/security/notices/USN-6797-1`
`cve: CVE-2023-22655`
`cve: CVE-2023-28746`
`cve: CVE-2023-38575`
`cve: CVE-2023-39368`
`cve: CVE-2023-43490`
`cve: CVE-2023-45733`
`cve: CVE-2023-45745`
`cve: CVE-2023-46103`
`cve: CVE-2023-47855`
`advisory_id: USN-6797-1`
`cert-bund: WID-SEC-2024-1294`
`cert-bund: WID-SEC-2024-1152`
`cert-bund: WID-SEC-2024-0619`
`cert-bund: WID-SEC-2024-0615`
`dfn-cert: DFN-CERT-2024-1448`
`dfn-cert: DFN-CERT-2024-1444`
`dfn-cert: DFN-CERT-2024-1314`
`dfn-cert: DFN-CERT-2024-1309`
`dfn-cert: DFN-CERT-2024-1304`
`dfn-cert: DFN-CERT-2024-1202`
`dfn-cert: DFN-CERT-2024-1173`
`dfn-cert: DFN-CERT-2024-1122`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-1023
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0910
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-2024-0770
dfn-cert: DFN-CERT-2024-0708
dfn-cert: DFN-CERT-2024-0690
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0678
dfn-cert: DFN-CERT-2024-0667
dfn-cert: DFN-CERT-2024-0666
dfn-cert: DFN-CERT-2024-0665
dfn-cert: DFN-CERT-2024-0628
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6664-1)

Summary
The remote host is missing an update for the 'less' package(s) announced via the USN-6664-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   less
Installed version:    less-551-1ubuntu0.1
Fixed version:      >=less-551-1ubuntu0.2
```

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

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

Vulnerability Insight
It was discovered that less incorrectly handled certain file names. An attacker could possibly use this issue to cause a crash or execute arbitrary commands.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6664-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6664.1
Version used: `2024-02-28T04:09:25Z`

References

```
url: https://ubuntu.com/security/notices/USN-6664-1
cve: CVE-2022-48624
advisory_id: USN-6664-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0434
dfn-cert: DFN-CERT-2024-1210
dfn-cert: DFN-CERT-2024-0532
```

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-551-1ubuntu0.1
Fixed version:      >=less-551-1ubuntu0.3
```

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
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.

... continues on next page ...

... continued from previous page ...

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: libc6-2.31-0ubuntu9.2
Fixed version: >=libc6-2.31-0ubuntu9.15

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.

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

... continues on next page ...

... continued from previous page ...

url: https://ubuntu.com/security/notices/USN-6737-1
cve: CVE-2024-2961
advisory_id: USN-6737-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-1226
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-6279-1)

Summary
The remote host is missing an update for the 'openssh' package(s) announced via the USN-6279-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: openssh-client
Installed version: openssh-client-1:8.2p1-4ubuntu0.2
Fixed version: >=openssh-client-1:8.2p1-4ubuntu0.9

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

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

Vulnerability Insight
It was discovered that OpenSSH has an observable discrepancy leading to an information leak in the algorithm negotiation. This update mitigates the issue by tweaking the client hostkey preference ordering algorithm to prefer the default ordering if the user has a key that matches the best-preference default algorithm.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6279-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6279.1
Version used: 2023-08-10T04:09:25Z

References
url: https://ubuntu.com/security/notices/USN-6279-1

... continues on next page ...

... continued from previous page ...

url: https://launchpad.net/bugs/2030275
advisory_id: USN-6279-1

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5060-1)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5060-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: ntfs-3g
Installed version: ntfs-3g-1:2017.3.23AR.3-3ubuntu1
Fixed version: >=ntfs-3g-1:2017.3.23AR.3-3ubuntu1.1

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that NTFS-3G incorrectly handled certain image file. An attacker could possibly use this issue to execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5060-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5060.1
Version used: 2022-09-13T14:14:11Z

References
url: https://ubuntu.com/security/notices/USN-5060-1
url: https://launchpad.net/bugs/1942235
advisory_id: USN-5060-1

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5745-2)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'shadow' package(s) announced via the USN-5745-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   login
Installed version:    login-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=login-1:4.8.1-1ubuntu5.20.04.4
Vulnerable package:   passwd
Installed version:    passwd-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=passwd-1:4.8.1-1ubuntu5.20.04.4
```

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

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

Vulnerability Insight
USN-5745-1 fixed vulnerabilities in shadow. Unfortunately that update introduced a regression that caused useradd to behave incorrectly in Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. This update reverts the security fix pending further investigation.
We apologize for the inconvenience.
Original advisory details:
Florian Weimer discovered that shadow was not properly copying and removing user directory trees, which could lead to a race condition. A local attacker could possibly use this issue to setup a symlink attack and alter or remove directories without authorization.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5745-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5745.2
Version used: `2022-11-30T04:11:02Z`

References

```
url: https://ubuntu.com/security/notices/USN-5745-2
url: https://launchpad.net/bugs/1998169
advisory_id: USN-5745-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5473-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5473-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20210119~20.04.1
Fixed version:      >=ca-certificates-20211016~20.04.1
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.50 version of the Mozilla certificate authority bundle.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5473-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5473.1
Version used: `2022-08-26T07:43:23Z`

References
```
url: https://ubuntu.com/security/notices/USN-5473-1
url: https://launchpad.net/bugs/1976631
advisory_id: USN-5473-1
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6543-1)

Summary
The remote host is missing an update for the 'tar' package(s) announced via the USN-6543-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   tar
```

... continues on next page ...

... continued from previous page ...

```
Installed version:    tar-1.30+dfsg-7ubuntu0.20.04.1
Fixed version:      >=tar-1.30+dfsg-7ubuntu0.20.04.4
```

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

Affected Software/OS
'tar' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that tar incorrectly handled extended attributes in PAX archives. An attacker could use this issue to cause tar to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6543-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6543.1
Version used: `2023-12-11T07:18:25Z`

References
`url: https://ubuntu.com/security/notices/USN-6543-1`
`cve: CVE-2023-39804`
`advisory_id: USN-6543-1`
`cert-bund: WID-SEC-2023-3093`
`dfn-cert: DFN-CERT-2024-0285`
`dfn-cert: DFN-CERT-2023-3074`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5761-1)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5761-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20210119~20.04.1
Fixed version:      >=ca-certificates-20211016ubuntu0.20.04.1
```

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

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

Vulnerability Insight
Due to security concerns, the TrustCor certificate authority has been marked as distrusted in Mozilla's root store. This update removes the TrustCor CA certificates from the ca-certificates package.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5761-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5761.1
Version used: `2022-12-06T04:10:22Z`

References
`url: https://ubuntu.com/security/notices/USN-5761-1`
`url: https://launchpad.net/bugs/1998785`
`advisory_id: USN-5761-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6105-1)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-6105-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20210119~20.04.1
Fixed version:      >=ca-certificates-20230311ubuntu0.20.04.1
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.60 version of the Mozilla certificate authority bundle.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6105-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6105.1
Version used: `2023-05-25T04:09:16Z`

References
`url: https://ubuntu.com/security/notices/USN-6105-1`
`url: https://launchpad.net/bugs/2020089`
`advisory_id: USN-6105-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6715-1)

Summary
The remote host is missing an update for the 'unixodbc' package(s) announced via the USN-6715-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libodbc1
Installed version:    libodbc1-2.3.6-0.1build1
Fixed version:      >=libodbc1-2.3.6-0.1ubuntu0.1
```

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

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

Vulnerability Insight
It was discovered that unixODBC incorrectly handled certain bytes. An attacker could use this issue to execute arbitrary code or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6715-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6715.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-03-28T04:09:04Z

References
url: https://ubuntu.com/security/notices/USN-6715-1
cve: CVE-2024-1013
advisory_id: USN-6715-1
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-0824

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6721-1)

Summary
The remote host is missing an update for the 'xorg-server, xwayland' package(s) announced via the USN-6721-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   xserver-xorg-core
Installed version:    xserver-xorg-core-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xserver-xorg-core-2:1.20.13-1ubuntu1~20.04.16
Vulnerable package:   xwayland
Installed version:    xwayland-2:1.20.9-2ubuntu1.2~20.04.2
Fixed version:      >=xwayland-2:1.20.13-1ubuntu1~20.04.16
```

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

Affected Software/OS
'xorg-server, xwayland' 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 X.Org X Server incorrectly handled certain data. An attacker could possibly use this issue to expose sensitive information. (CVE-2024-31080, CVE-2024-31081, CVE-2024-31082)
It was discovered that X.Org X Server incorrectly handled certain glyphs. An attacker could possibly use this issue to cause a crash or expose sensitive information. (CVE-2024-31083)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6721-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6721.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-04-08T04:09:12Z

References
url: https://ubuntu.com/security/notices/USN-6721-1
cve: CVE-2024-31080
cve: CVE-2024-31081
cve: CVE-2024-31082
cve: CVE-2024-31083
advisory_id: USN-6721-1
cert-bund: WID-SEC-2024-0778
dfn-cert: DFN-CERT-2024-0982
dfn-cert: DFN-CERT-2024-0976
dfn-cert: DFN-CERT-2024-0877

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6649-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6649-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-123.0+build3-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1557)
Alfred Peters discovered that Firefox did not properly manage memory when storing and re-accessing data on a networking channel. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1546)

... continues on next page ...

... continued from previous page ...

Johan Carlsson discovered that Firefox incorrectly handled Set-Cookie response headers in multipart HTTP responses. An attacker could potentially exploit this issue to inject arbitrary cookie values. (CVE-2024-1551)
Gary Kwong discovered that Firefox incorrectly generated codes on 32-bit ARM devices, which could lead to unexpected numeric conversions or undefined behaviour. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-1552)
Ronald Crane discovered that Firefox did not properly manage memory when accessing the built-in profiler. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1556)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6649-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6649.1
Version used: `2024-02-22T10:31:46Z`

References
`url: https://ubuntu.com/security/notices/USN-6649-1`
`cve: CVE-2024-1546`
`cve: CVE-2024-1547`
`cve: CVE-2024-1548`
`cve: CVE-2024-1549`
`cve: CVE-2024-1550`
`cve: CVE-2024-1551`
`cve: CVE-2024-1552`
`cve: CVE-2024-1553`
`cve: CVE-2024-1554`
`cve: CVE-2024-1555`
`cve: CVE-2024-1556`
`cve: CVE-2024-1557`
`advisory_id: USN-6649-1`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0443`
`dfn-cert: DFN-CERT-2024-0815`
`dfn-cert: DFN-CERT-2024-0562`
`dfn-cert: DFN-CERT-2024-0455`
`dfn-cert: DFN-CERT-2024-0449`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6649-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6649-2 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-123.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6649-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1557)
Alfred Peters discovered that Firefox did not properly manage memory when storing and re-accessing data on a networking channel. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1546)
Johan Carlsson discovered that Firefox incorrectly handled Set-Cookie response headers in multipart HTTP responses. An attacker could potentially exploit this issue to inject arbitrary cookie values. (CVE-2024-1551)
Gary Kwong discovered that Firefox incorrectly generated codes on 32-bit ARM devices, which could lead to unexpected numeric conversions or undefined behaviour. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-1552)
Ronald Crane discovered that Firefox did not properly manage memory when accessing the built-in profiler. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-1556)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6649-2)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6649.2
Version used: 2024-03-06T08:59:21Z

References
url: https://ubuntu.com/security/notices/USN-6649-2
url: https://launchpad.net/bugs/2056258
cve: CVE-2024-1546
cve: CVE-2024-1547

... continues on next page ...

... continued from previous page ...

cve: CVE-2024-1548
cve: CVE-2024-1549
cve: CVE-2024-1550
cve: CVE-2024-1551
cve: CVE-2024-1552
cve: CVE-2024-1553
cve: CVE-2024-1554
cve: CVE-2024-1555
cve: CVE-2024-1556
cve: CVE-2024-1557
advisory_id: USN-6649-2
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-0443
dfn-cert: DFN-CERT-2024-0815
dfn-cert: DFN-CERT-2024-0562
dfn-cert: DFN-CERT-2024-0455
dfn-cert: DFN-CERT-2024-0449

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6703-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6703-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-124.0+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-2609, CVE-2024-2611, CVE-2024-2614, CVE-2024-2615)

... continues on next page ...

... continued from previous page ...

Hubert Kario discovered that Firefox had a timing side-channel when performing RSA decryption. A remote attacker could possibly use this issue to recover sensitive information. (CVE-2023-5388)
It was discovered that Firefox did not properly handle WASM register values in some circumstances. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2606)
Gary Kwong discovered that Firefox incorrectly updated return registers for JIT code on Armv7-A systems. An attacker could potentially exploit this issue to execute arbitrary code. (CVE-2024-2607)
Ronald Crane discovered that Firefox did not properly manage memory during character encoding. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2608)
Georg Felber and Marco Squarcina discovered that Firefox incorrectly handled html and body tags. An attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able obtain sensitive information. (CVE-2024-2610)
Ronald Crane discovered a use-after-free in Firefox when handling code in SafeRefPtr. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-2612)
Max Inden discovered that Firefox incorrectly handled QUIC ACK frame decoding. A attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-2613)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6703-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6703.1
Version used: `2024-03-21T04:09:31Z`

References
`url: https://ubuntu.com/security/notices/USN-6703-1`
`cve: CVE-2023-5388`
`cve: CVE-2024-2606`
`cve: CVE-2024-2607`
`cve: CVE-2024-2608`
`cve: CVE-2024-2609`
`cve: CVE-2024-2610`
`cve: CVE-2024-2611`
`cve: CVE-2024-2612`
`cve: CVE-2024-2613`
`cve: CVE-2024-2614`
`cve: CVE-2024-2615`
`advisory_id: USN-6703-1`
`cert-bund: WID-SEC-2024-1351`
`cert-bund: WID-SEC-2024-1248`
`cert-bund: WID-SEC-2024-0669`
`cert-bund: WID-SEC-2024-0045`
`dfn-cert: DFN-CERT-2024-1071`
`dfn-cert: DFN-CERT-2024-1050`
`dfn-cert: DFN-CERT-2024-1011`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1008
dfn-cert: DFN-CERT-2024-0955
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-2024-0069

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6710-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6710-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-124.0.1+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Manfred Paul discovered that Firefox did not properly perform bounds checking during range analysis, leading to an out-of-bounds write vulnerability. A attacker could use this to cause a denial of service, or execute arbitrary code. (CVE-2024-29943)
Manfred Paul discovered that Firefox incorrectly handled MessageManager listeners under certain circumstances. An attacker who was able to inject an event handler into a privileged object may have been able to execute arbitrary code. (CVE-2024-29944)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6710-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6710.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-03-25T08:40:03Z

References

url: https://ubuntu.com/security/notices/USN-6710-1
cve: CVE-2024-29943
cve: CVE-2024-29944
advisory_id: USN-6710-1
cert-bund: WID-SEC-2024-0703
dfn-cert: DFN-CERT-2024-0815
dfn-cert: DFN-CERT-2024-0796
dfn-cert: DFN-CERT-2024-0768

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6710-2)

Summary

The remote host is missing an update for the 'firefox' package(s) announced via the USN-6710-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-124.0.2+build1-0ubuntu0.20.04.1

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight

USN-6710-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Original advisory details:

Manfred Paul discovered that Firefox did not properly perform bounds checking during range analysis, leading to an out-of-bounds write vulnerability. A attacker could use this to cause a denial of service, or execute arbitrary code. (CVE-2024-29943)

Manfred Paul discovered that Firefox incorrectly handled MessageManager listeners under certain circumstances. An attacker who was able to inject an event handler into a privileged object may have been able to execute arbitrary code. (CVE-2024-29944)

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6710-2)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6710.2
Version used: 2024-04-05T04:09:49Z

References
url: https://ubuntu.com/security/notices/USN-6710-2
url: https://launchpad.net/bugs/2060171
cve: CVE-2024-29943
cve: CVE-2024-29944
advisory_id: USN-6710-2
cert-bund: WID-SEC-2024-0703
dfn-cert: DFN-CERT-2024-0815
dfn-cert: DFN-CERT-2024-0796
dfn-cert: DFN-CERT-2024-0768

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6747-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6747-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-125.0.2+build1-0ubuntu0.20.04.2

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-3852, CVE-2024-3864, CVE-2024-3865)
Bartek Nowotarski discovered that Firefox did not properly limit HTTP/2 CONTINUATION frames. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3302)

... continues on next page ...

... continued from previous page ...

Gary Kwong discovered that Firefox did not properly manage memory when running garbage collection during realm initialization. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3853)
Lukas Bernhard discovered that Firefox did not properly manage memory during JIT optimisations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3854, CVE-2024-3855)
Nan Wang discovered that Firefox did not properly manage memory during WASM garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3856)
Lukas Bernhard discovered that Firefox did not properly manage memory when handling JIT created code during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3857)
Lukas Bernhard discovered that Firefox did not properly manage memory when tracing in JIT. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3858)
Ronald Crane discovered that Firefox did not properly manage memory in the OpenType sanitizer on 32-bit devices, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3859)
Garry Kwong discovered that Firefox did not properly manage memory when tracing empty shape lists in JIT. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3860)
Ronald Crane discovered that Firefox did not properly manage memory when handling an AlignedBuffer. An attacker could potentially exploit this issue to cause denial of service, or execute arbitrary code. (CVE-2024-3861)
Ronald Crane discovered that Firefox did not properly manage memory when handling code in MarkStack. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-3862)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6747-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6747.1
Version used: `2024-04-25T04:09:16Z`

References
`url: https://ubuntu.com/security/notices/USN-6747-1`
`cve: CVE-2024-3302`
`cve: CVE-2024-3852`
`cve: CVE-2024-3853`
`cve: CVE-2024-3854`
`cve: CVE-2024-3855`
`cve: CVE-2024-3856`
`cve: CVE-2024-3857`
`cve: CVE-2024-3858`
`cve: CVE-2024-3859`
`cve: CVE-2024-3860`
`cve: CVE-2024-3861`
`cve: CVE-2024-3862`

... continues on next page ...

... continued from previous page ...

cve: CVE-2024-3864
cve: CVE-2024-3865
advisory_id: USN-6747-1
cert-bund: WID-SEC-2024-0909
dfn-cert: DFN-CERT-2024-1050
dfn-cert: DFN-CERT-2024-1008

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6747-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6747-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

Vulnerable package:	firefox
Installed version:	firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:	>=firefox-125.0.3+build1-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
USN-6747-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-3852, CVE-2024-3864, CVE-2024-3865)
Bartek Nowotarski discovered that Firefox did not properly limit HTTP/2 CONTINUATION frames. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3302)
Gary Kwong discovered that Firefox did not properly manage memory when running garbage collection during realm initialization. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3853)
Lukas Bernhard discovered that Firefox did not properly manage memory during JIT optimisations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3854, CVE-2024-3855)

... continues on next page ...

... continued from previous page ...

Nan Wang discovered that Firefox did not properly manage memory during WASM garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3856)
Lukas Bernhard discovered that Firefox did not properly manage memory when handling JIT created code during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3857)
Lukas Bernhard discovered that Firefox did not properly manage memory when tracing in JIT. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3858)
Ronald Crane discovered that Firefox did not properly manage memory in the OpenType sanitizer on 32-bit devices, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3859)
Garry Kwong discovered that Firefox did not properly manage memory when tracing empty shape lists in JIT. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3860)
Ronald Crane discovered that Firefox did not properly manage memory when handling an AlignedBuffer. An attacker could potentially exploit this issue to cause denial of service, or execute arbitrary code. (CVE-2024-3861)
Ronald Crane discovered that Firefox did not properly manage memory when handling code in MarkStack. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-3862)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6747-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6747.2
Version used: `2024-05-02T11:46:08Z`

References
`url: https://ubuntu.com/security/notices/USN-6747-2`
`url: https://launchpad.net/bugs/2064553`
`cve: CVE-2024-3302`
`cve: CVE-2024-3852`
`cve: CVE-2024-3853`
`cve: CVE-2024-3854`
`cve: CVE-2024-3855`
`cve: CVE-2024-3856`
`cve: CVE-2024-3857`
`cve: CVE-2024-3858`
`cve: CVE-2024-3859`
`cve: CVE-2024-3860`
`cve: CVE-2024-3861`
`cve: CVE-2024-3862`
`cve: CVE-2024-3864`
`cve: CVE-2024-3865`
`advisory_id: USN-6747-2`
`cert-bund: WID-SEC-2024-0909`
`dfn-cert: DFN-CERT-2024-1050`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1008

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6779-1)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6779-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: firefox
Installed version: firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version: >=firefox-126.0+build2-0ubuntu0.20.04.1

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4771, CVE-2024-4772, CVE-2024-4773, CVE-2024-4774, CVE-2024-4775, CVE-2024-4776, CVE-2024-4777, CVE-2024-4778)
Jan-Ivar Bruaroey discovered that Firefox did not properly manage memory when audio input connected with multiple consumers. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-4764)
Thomas Rinsma discovered that Firefox did not properly handle type check when handling fonts in PDF.js. An attacker could potentially exploit this issue to execute arbitrary javascript code in PDF.js. (CVE-2024-4367)
Irvan Kurniawan discovered that Firefox did not properly handle certain font styles when saving a page to PDF. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-4770)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6779-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6779.1
Version used: 2024-05-22T04:08:02Z

... continues on next page ...

... continued from previous page ...

References

```
url: https://ubuntu.com/security/notices/USN-6779-1
cve: CVE-2024-4367
cve: CVE-2024-4764
cve: CVE-2024-4767
cve: CVE-2024-4768
cve: CVE-2024-4769
cve: CVE-2024-4770
cve: CVE-2024-4771
cve: CVE-2024-4772
cve: CVE-2024-4773
cve: CVE-2024-4774
cve: CVE-2024-4775
cve: CVE-2024-4776
cve: CVE-2024-4777
cve: CVE-2024-4778
advisory_id: USN-6779-1
cert-bund: WID-SEC-2024-1216
cert-bund: WID-SEC-2024-1151
dfn-cert: DFN-CERT-2024-1374
dfn-cert: DFN-CERT-2024-1290
dfn-cert: DFN-CERT-2024-1284
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6779-2)

Summary
The remote host is missing an update for the 'firefox' package(s) announced via the USN-6779-2 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   firefox
Installed version:    firefox-89.0.1+build1-0ubuntu0.20.04.1
Fixed version:      >=firefox-126.0.1+build1-0ubuntu0.20.04.1
```

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

Affected Software/OS
'firefox' package(s) on Ubuntu 20.04.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

USN-6779-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.
Original advisory details:
Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. (CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4771, CVE-2024-4772, CVE-2024-4773, CVE-2024-4774, CVE-2024-4775, CVE-2024-4776, CVE-2024-4777, CVE-2024-4778)
Jan-Ivar Bruaroey discovered that Firefox did not properly manage memory when audio input connected with multiple consumers. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-4764)
Thomas Rinsma discovered that Firefox did not properly handle type check when handling fonts in PDF.js. An attacker could potentially exploit this issue to execute arbitrary javascript code in PDF.js. (CVE-2024-4367)
Irvan Kurniawan discovered that Firefox did not properly handle certain font styles when saving a page to PDF. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-4770)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6779-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6779.2
Version used: `2024-05-30T04:08:53Z`

References
`url: https://ubuntu.com/security/notices/USN-6779-2`
`url: https://launchpad.net/bugs/2067445`
`cve: CVE-2024-4367`
`cve: CVE-2024-4764`
`cve: CVE-2024-4767`
`cve: CVE-2024-4768`
`cve: CVE-2024-4769`
`cve: CVE-2024-4770`
`cve: CVE-2024-4771`
`cve: CVE-2024-4772`
`cve: CVE-2024-4773`
`cve: CVE-2024-4774`
`cve: CVE-2024-4775`
`cve: CVE-2024-4776`
`cve: CVE-2024-4777`
`cve: CVE-2024-4778`
`advisory_id: USN-6779-2`
`cert-bund: WID-SEC-2024-1216`
`cert-bund: WID-SEC-2024-1151`
`dfn-cert: DFN-CERT-2024-1374`
`dfn-cert: DFN-CERT-2024-1290`
`dfn-cert: DFN-CERT-2024-1284`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5089-1)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5089-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20210119~20.04.1
Fixed version:      >=ca-certificates-20210119~20.04.2
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
The ca-certificates package contained a CA certificate that will expire on 2021-09-30 and will cause connectivity issues. This update removes the 'DST Root CA X3' CA.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5089-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5089.1
Version used: `2022-08-26T07:43:23Z`

References
```
url: https://ubuntu.com/security/notices/USN-5089-1
url: https://launchpad.net/bugs/1944481
advisory_id: USN-5089-1
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5028-1)

Summary
The remote host is missing an update for the 'exiv2' package(s) announced via the USN-5028-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

Vulnerable package: libexiv2-27
Installed version: libexiv2-27-0.27.2-8ubuntu2.4
Fixed version: >=libexiv2-27-0.27.2-8ubuntu2.5

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

Affected Software/OS
'exiv2' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that Exiv2 incorrectly handled certain images. 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-5028-1)
OID:1.3.6.1.4.1.25623.1.1.12.2021.5028.1
Version used: 2022-09-13T14:14:11Z

References
url: https://ubuntu.com/security/notices/USN-5028-1
cve: CVE-2021-31291
advisory_id: USN-5028-1
cert-bund: WID-SEC-2022-1640
cert-bund: CB-K21/0872
dfn-cert: DFN-CERT-2022-2697
dfn-cert: DFN-CERT-2022-2491
dfn-cert: DFN-CERT-2022-2290
dfn-cert: DFN-CERT-2022-2217
dfn-cert: DFN-CERT-2021-1733
dfn-cert: DFN-CERT-2021-1639

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5441-1)

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the USN-5441-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libjavascriptcoregtk-4.0-18

... continues on next page ...

... continued from previous page ...

```
Installed version:    libjavascriptcoregtk-4.0-18-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libjavascriptcoregtk-4.0-18-2.36.2-0ubuntu0.20.04.1
Vulnerable package:   libwebkit2gtk-4.0-37
Installed version:    libwebkit2gtk-4.0-37-2.32.0-0ubuntu0.20.04.1
Fixed version:      >=libwebkit2gtk-4.0-37-2.36.2-0ubuntu0.20.04.1
```

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

Affected Software/OS
'webkit2gtk' package(s) on Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
A large number of 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-5441-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5441.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5441-1`
`url: https://launchpad.net/bugs/1975602`
`advisory_id: USN-5441-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5543-1)

Summary
The remote host is missing an update for the 'net-snmp' package(s) announced via the USN-5543-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libsnmp35
Installed version:    libsnmp35-5.8+dfsg-2ubuntu2.3
Fixed version:      >=libsnmp35-5.8+dfsg-2ubuntu2.4
```

Solution:

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
Yu Zhang and Nanyu Zhong discovered that Net-SNMP incorrectly handled memory operations when processing certain requests. A remote attacker could use this issue to cause Net-SNMP to crash, resulting in 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-5543-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5543.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5543-1`
`cve: CVE-2022-24805`
`cve: CVE-2022-24806`
`cve: CVE-2022-24807`
`cve: CVE-2022-24808`
`cve: CVE-2022-24809`
`cve: CVE-2022-24810`
`advisory_id: USN-5543-1`
`cert-bund: WID-SEC-2022-0604`
`dfn-cert: DFN-CERT-2022-1690`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6663-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-6663-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libssl1.1
Installed version:    libssl1.1-1.1.1f-1ubuntu2.4
Fixed version:      >=libssl1.1-1.1.1f-1ubuntu2.22
Vulnerable package:   openssl
Installed version:    openssl-1.1.1f-1ubuntu2.4
Fixed version:      >=openssl-1.1.1f-1ubuntu2.22
```

... continues on next page ...

... continued from previous page ...

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 23.10.

Vulnerability Insight
As a security improvement, OpenSSL will now return deterministic random bytes instead of an error when detecting wrong padding in PKCS#1 v1.5 RSA to prevent its use in possible Bleichenbacher timing attacks.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6663-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6663.1
Version used: `2024-02-28T04:09:25Z`

References
`url: https://ubuntu.com/security/notices/USN-6663-1`
`url: https://launchpad.net/bugs/2054090`
`advisory_id: USN-6663-1`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6750-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6750-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:115.10.1+build1-0ubuntu0.20.04.1
```

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

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

... continues on next page ...

... continued from previous page ...

Vulnerability Insight

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-2609, CVE-2024-3852, CVE-2024-3864)

Bartek Nowotarski discovered that Thunderbird did not properly limit HTTP/2 CONTINUATION frames. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-3302)

Lukas Bernhard discovered that Thunderbird did not properly manage memory during JIT optimisations, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3854)

Lukas Bernhard discovered that Thunderbird did not properly manage memory when handling JIT created code during garbage collection. An attacker could potentially exploit this issue to cause a denial of service, or execute arbitrary code. (CVE-2024-3857)

Ronald Crane discovered that Thunderbird did not properly manage memory in the OpenType sanitizer on 32-bit devices, leading to an out-of-bounds read vulnerability. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. (CVE-2024-3859)

Ronald Crane discovered that Thunderbird did not properly manage memory when handling an AlignedBuffer. An attacker could potentially exploit this issue to cause denial of service, or execute arbitrary code. (CVE-2024-3861)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-6750-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2024.6750.1

Version used: `2024-04-26T04:09:00Z`

References

`url: https://ubuntu.com/security/notices/USN-6750-1`
`cve: CVE-2024-2609`
`cve: CVE-2024-3302`
`cve: CVE-2024-3852`
`cve: CVE-2024-3854`
`cve: CVE-2024-3857`
`cve: CVE-2024-3859`
`cve: CVE-2024-3861`
`cve: CVE-2024-3864`
`advisory_id: USN-6750-1`
`cert-bund: WID-SEC-2024-1351`
`cert-bund: WID-SEC-2024-0909`
`cert-bund: WID-SEC-2024-0669`
`dfn-cert: DFN-CERT-2024-1050`
`dfn-cert: DFN-CERT-2024-1008`
`dfn-cert: DFN-CERT-2024-0734`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6568-1)

Summary
The remote host is missing an update for the 'clamav' package(s) announced via the USN-6568-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   clamav
Installed version:    clamav-0.103.2+dfsg-0ubuntu0.20.04.2
Fixed version:      >=clamav-0.103.11+dfsg-0ubuntu0.20.04.1
```

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

Affected Software/OS
'clamav' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
The ClamAV package was updated to a new upstream version to remain compatible with signature database downloads.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6568-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6568.1
Version used: `2024-01-09T04:08:55Z`

References
```
url: https://ubuntu.com/security/notices/USN-6568-1
url: https://launchpad.net/bugs/2046581
advisory_id: USN-6568-1
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6676-1)

Summary
The remote host is missing an update for the 'c-ares' package(s) announced via the USN-6676-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

Vulnerable package: libc-ares2
Installed version: libc-ares2-1.15.0-1build1
Fixed version: >=libc-ares2-1.15.0-1ubuntu0.5

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

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

Vulnerability Insight
Vojtech Vobr discovered that c-ares incorrectly handled user input from local configuration files. An attacker could possibly use this issue to cause a denial of service via application crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6676-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6676.1
Version used: 2024-03-07T04:08:56Z

References
url: https://ubuntu.com/security/notices/USN-6676-1
cve: CVE-2024-25629
advisory_id: USN-6676-1
cert-bund: WID-SEC-2024-1337
cert-bund: WID-SEC-2024-0992
dfn-cert: DFN-CERT-2024-1413
dfn-cert: DFN-CERT-2024-1252
dfn-cert: DFN-CERT-2024-0591

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6744-1)

Summary
The remote host is missing an update for the 'pillow' package(s) announced via the USN-6744-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: python3-pil
Installed version: python3-pil-7.0.0-4ubuntu0.4
Fixed version: >=python3-pil-7.0.0-4ubuntu0.9

... continues on next page ...

... continued from previous page ...

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

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

Vulnerability Insight
Hugo van Kemenade discovered that Pillow was not properly performing bounds checks when processing an ICC file, which could lead to a buffer overflow. If a user or automated system were tricked into processing a specially crafted ICC file, an attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6744-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6744.1
Version used: `2024-04-24T04:09:36Z`

References
`url: https://ubuntu.com/security/notices/USN-6744-1`
`cve: CVE-2024-28219`
`advisory_id: USN-6744-1`
`cert-bund: WID-SEC-2024-1328`
`dfn-cert: DFN-CERT-2024-1483`
`dfn-cert: DFN-CERT-2024-0865`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5376-3)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5376-3 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   git
Installed version:    git-1:2.25.1-1ubuntu3.1
Fixed version:      >=git-1:2.25.1-1ubuntu3.4
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'git' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10, Ubuntu 22.04.

Vulnerability Insight
USN-5376-1 fixed vulnerabilities in Git, some patches were missing to properly fix the issue. This update fixes the problem.
Original advisory details:
Yu Chen Dong discovered that Git incorrectly handled certain repository paths in platforms with multiple users support. An attacker could possibly use this issue to run arbitrary commands.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5376-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5376.3
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5376-3`
`url: https://launchpad.net/bugs/1970260`
`advisory_id: USN-5376-3`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6782-1)

Summary
The remote host is missing an update for the 'thunderbird' package(s) announced via the USN-6782-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   thunderbird
Installed version:    thunderbird-1:78.11.0+build1-0ubuntu0.20.04.2
Fixed version:      >=thunderbird-1:115.11.0+build2-0ubuntu0.20.04.1
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code. (CVE-2024-4767, CVE-2024-4768, CVE-2024-4769, CVE-2024-4777)
Thomas Rinsma discovered that Thunderbird did not properly handle type check when handling fonts in PDF.js. An attacker could potentially exploit this issue to execute arbitrary javascript code in PDF.js. (CVE-2024-4367)
Irvan Kurniawan discovered that Thunderbird did not properly handle certain font styles when saving a page to PDF. An attacker could potentially exploit this issue to cause a denial of service. (CVE-2024-4770)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6782-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6782.1
Version used: `2024-05-23T04:07:41Z`

References
`url: https://ubuntu.com/security/notices/USN-6782-1`
`cve: CVE-2024-4367`
`cve: CVE-2024-4767`
`cve: CVE-2024-4768`
`cve: CVE-2024-4769`
`cve: CVE-2024-4770`
`cve: CVE-2024-4777`
`advisory_id: USN-6782-1`
`cert-bund: WID-SEC-2024-1216`
`cert-bund: WID-SEC-2024-1151`
`dfn-cert: DFN-CERT-2024-1374`
`dfn-cert: DFN-CERT-2024-1290`
`dfn-cert: DFN-CERT-2024-1284`

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:    libgnutls30-3.6.13-2ubuntu1.3
Fixed version:      >=libgnutls30-3.6.13-2ubuntu1.11
```

... continues on next page ...

... continued from previous page ...

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)`
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-2024-1307`
`cert-bund: WID-SEC-2024-1226`
`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`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6718-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-6718-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.22
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.22
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.22
```

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

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

Vulnerability Insight
Dan Fandrich discovered that curl would incorrectly use the default set of protocols when a parameter option disabled all protocols without adding any, contrary to expectations. This issue only affected Ubuntu 23.10. (CVE-2024-2004)
It was discovered that curl incorrectly handled memory when limiting the amount of headers when HTTP/2 server push is allowed. A remote attacker could possibly use this issue to cause curl to consume resources, leading to a denial of service. (CVE-2024-2398)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6718-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6718.1
Version used: `2024-03-28T04:09:04Z`

References

```
url: https://ubuntu.com/security/notices/USN-6718-1
cve: CVE-2024-2004
cve: CVE-2024-2398
advisory_id: USN-6718-1
cert-bund: WID-SEC-2024-0726
dfn-cert: DFN-CERT-2024-1238
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-0825
dfn-cert: DFN-CERT-2024-0817
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6814-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'libvpx' package(s) announced via the USN-6814-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libvpx6
Installed version:    libvpx6-1.8.2-1build1
Fixed version:      >=libvpx6-1.8.2-1ubuntu0.3
```

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

Affected Software/OS
'libvpx' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Xiantong Hou discovered that libvpx did not properly handle certain malformed media files. If an application using libvpx opened a specially crafted file, a remote attacker could 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-6814-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6814.1
Version used: `2024-06-07T04:08:49Z`

References
```
url: https://ubuntu.com/security/notices/USN-6814-1
cve: CVE-2024-5197
advisory_id: USN-6814-1
dfn-cert: DFN-CERT-2024-1488
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6833-1)

Summary
The remote host is missing an update for the 'vte2.91' package(s) announced via the USN-6833-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   libvte-2.91-0
Installed version:    libvte-2.91-0-0.60.3-0ubuntu1~20.04
Fixed version:      >=libvte-2.91-0-0.60.3-0ubuntu1~20.5
```

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

Affected Software/OS
'vte2.91' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Siddharth Dushantha discovered that VTE incorrectly handled large window resize escape sequences. An attacker could possibly use this issue to consume resources, leading to a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6833-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6833.1
Version used: `2024-06-14T04:07:51Z`

References
`url: https://ubuntu.com/security/notices/USN-6833-1`
`cve: CVE-2024-37535`
`advisory_id: USN-6833-1`

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:    libglib2.0-0-2.64.6-1~ubuntu20.04.3
Fixed version:      >=libglib2.0-0-2.64.6-1~ubuntu20.04.7
Vulnerable package:   libglib2.0-bin
Installed version:    libglib2.0-bin-2.64.6-1~ubuntu20.04.3
Fixed version:      >=libglib2.0-bin-2.64.6-1~ubuntu20.04.7
```

Solution:

... continues on next page ...

... continued from previous page ...

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.

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-6787-1)

Summary
The remote host is missing an update for the 'jinja2' package(s) announced via the USN-6787-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-jinja2
Installed version:    python3-jinja2-2.10.1-2
Fixed version:      >=python3-jinja2-2.10.1-2ubuntu0.3
```

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

Affected Software/OS
'jinja2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
It was discovered that Jinja2 incorrectly handled certain HTML attributes that were accepted by the xmlattr filter. An attacker could use this issue to inject arbitrary HTML attribute keys and values to potentially execute a cross-site scripting (XSS) attack.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6787-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6787.1
Version used: `2024-05-29T04:09:43Z`

References
`url: https://ubuntu.com/security/notices/USN-6787-1`
`cve: CVE-2024-34064`
`advisory_id: USN-6787-1`
`cert-bund: WID-SEC-2024-1328`
`dfn-cert: DFN-CERT-2024-1334`
`dfn-cert: DFN-CERT-2024-1232`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6554-1)

Summary
The remote host is missing an update for the 'gnome-control-center' package(s) announced via the USN-6554-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   gnome-control-center
Installed version:    gnome-control-center-1:3.36.5-0ubuntu2
Fixed version:      >=gnome-control-center-1:3.36.5-0ubuntu4.1
```

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

Affected Software/OS
'gnome-control-center' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
Zygmunt Krynicki discovered that GNOME Settings did not accurately reflect the SSH remote login status when the system was configured to use systemd socket activation for OpenSSH. Remote SSH access may be unknowingly enabled, contrary to expectation.

... 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-6554-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6554.1
Version used: `2023-12-14T04:08:36Z`

References
`url: https://ubuntu.com/security/notices/USN-6554-1`
`cve: CVE-2023-5616`
`advisory_id: USN-6554-1`
`dfn-cert: DFN-CERT-2023-3101`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6803-1)

Summary
The remote host is missing an update for the 'ffmpeg' package(s) announced via the USN-6803-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libavcodec58
Installed version:    libavcodec58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavcodec58-7:4.2.7-0ubuntu0.1+esm5
Vulnerable package:   libavformat58
Installed version:    libavformat58-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavformat58-7:4.2.7-0ubuntu0.1+esm5
Vulnerable package:   libavutil56
Installed version:    libavutil56-7:4.2.4-1ubuntu0.1
Fixed version:      >=libavutil56-7:4.2.7-0ubuntu0.1+esm5
Vulnerable package:   libpostproc55
Installed version:    libpostproc55-7:4.2.4-1ubuntu0.1
Fixed version:      >=libpostproc55-7:4.2.7-0ubuntu0.1+esm5
Vulnerable package:   libswresample3
Installed version:    libswresample3-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswresample3-7:4.2.7-0ubuntu0.1+esm5
Vulnerable package:   libswscale5
Installed version:    libswscale5-7:4.2.4-1ubuntu0.1
Fixed version:      >=libswscale5-7:4.2.7-0ubuntu0.1+esm5
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'ffmpeg' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 24.04 LTS. (CVE-2023-49501)
Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-49502)
Zhang Ling and Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-49528)
Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-50007)
Zeng Yunxiang and Song Jiaxuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-50008)
Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10. (CVE-2023-50009)
Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-50010)
Zeng Yunxiang and Li Zeyuan discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2023-51793)
Zeng Yunxiang discovered that FFmpeg incorrectly handled certain input files. An attacker could possibly use this issue to cause FFmpeg to crash, resulting in a denial of service, or potential arbitrary code execution. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-51794, CVE-2023-51798)
Zeng Yunxiang discovered that FFmpeg incorrectly ... [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-6803-1)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.1.12.2024.6803.1
Version used: 2024-05-31T04:08:03Z

References

```
url: https://ubuntu.com/security/notices/USN-6803-1
cve: CVE-2023-49501
cve: CVE-2023-49502
cve: CVE-2023-49528
cve: CVE-2023-50007
cve: CVE-2023-50008
cve: CVE-2023-50009
cve: CVE-2023-50010
cve: CVE-2023-51793
cve: CVE-2023-51794
cve: CVE-2023-51795
cve: CVE-2023-51796
cve: CVE-2023-51798
cve: CVE-2024-31578
cve: CVE-2024-31582
cve: CVE-2024-31585
advisory_id: USN-6803-1
cert-bund: WID-SEC-2024-0982
cert-bund: WID-SEC-2024-0939
cert-bund: WID-SEC-2024-0923
cert-bund: WID-SEC-2024-0856
dfn-cert: DFN-CERT-2024-1465
dfn-cert: DFN-CERT-2024-1464
dfn-cert: DFN-CERT-2024-1446
dfn-cert: DFN-CERT-2024-1258
dfn-cert: DFN-CERT-2024-1135
dfn-cert: DFN-CERT-2024-1134
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6268-1)

Summary

The remote host is missing an update for the 'gst-plugins-base1.0' package(s) announced via the USN-6268-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   gstreamer1.0-plugins-base
Installed version:    gstreamer1.0-plugins-base-1.16.2-4ubuntu0.1
Fixed version:      >=gstreamer1.0-plugins-base-1.16.3-0ubuntu1.2
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'gst-plugins-base1.0' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that GStreamer Base Plugins incorrectly handled certain FLAC image tags. A remote attacker could use this issue to cause GStreamer Base Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37327)
It was discovered that GStreamer Base Plugins incorrectly handled certain subtitles. A remote attacker could use this issue to cause GStreamer Base Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37328)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6268-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6268.1
Version used: `2023-08-03T04:09:35Z`

References
`url: https://ubuntu.com/security/notices/USN-6268-1`
`cve: CVE-2023-37327`
`cve: CVE-2023-37328`
`advisory_id: USN-6268-1`
`cert-bund: WID-SEC-2023-1522`
`dfn-cert: DFN-CERT-2024-1162`
`dfn-cert: DFN-CERT-2023-3165`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-2306`
`dfn-cert: DFN-CERT-2023-2206`
`dfn-cert: DFN-CERT-2023-1813`
`dfn-cert: DFN-CERT-2023-1783`
`dfn-cert: DFN-CERT-2023-1689`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6798-1)

Summary
The remote host is missing an update for the 'gst-plugins-base1.0' package(s) announced via the USN-6798-1 advisory.

Quality of Detection: 97

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerable package: gstreamer1.0-plugins-base
Installed version: gstreamer1.0-plugins-base-1.16.2-4ubuntu0.1
Fixed version: >=gstreamer1.0-plugins-base-1.16.3-0ubuntu1.3

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

Affected Software/OS
'gst-plugins-base1.0' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
It was discovered that GStreamer Base Plugins incorrectly handled certain EXIF metadata. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6798-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6798.1
Version used: 2024-05-30T04:08:53Z

References
url: https://ubuntu.com/security/notices/USN-6798-1
cve: CVE-2024-4453
advisory_id: USN-6798-1
cert-bund: WID-SEC-2024-1209
dfn-cert: DFN-CERT-2024-1431

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6062-1)

Summary
The remote host is missing an update for the 'freetype' package(s) announced via the USN-6062-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libfreetype6
Installed version: libfreetype6-2.10.1-2ubuntu0.1
Fixed version: >=libfreetype6-2.10.1-2ubuntu0.3

Solution:
Solution type: VendorFix

... continues on next page ...

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS
'freetype' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10, Ubuntu 23.04.

Vulnerability Insight
It was discovered that FreeType incorrectly handled certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, 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-6062-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6062.1
Version used: `2023-05-29T04:09:36Z`

References
`url: https://ubuntu.com/security/notices/USN-6062-1`
`cve: CVE-2023-2004`
`advisory_id: USN-6062-1`
`cert-bund: WID-SEC-2023-2917`
`cert-bund: WID-SEC-2023-0961`
`dfn-cert: DFN-CERT-2023-2560`
`dfn-cert: DFN-CERT-2023-2558`
`dfn-cert: DFN-CERT-2023-1947`
`dfn-cert: DFN-CERT-2023-0913`
`dfn-cert: DFN-CERT-2023-0837`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6269-1)

Summary
The remote host is missing an update for the 'gst-plugins-good1.0' package(s) announced via the USN-6269-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   gstreamer1.0-plugins-good
Installed version:    gstreamer1.0-plugins-good-1.16.2-1ubuntu2.1
Fixed version:      >=gstreamer1.0-plugins-good-1.16.3-0ubuntu1.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'gst-plugins-good1.0' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that GStreamer Good Plugins incorrectly handled certain FLAC image tags. A remote attacker could use this issue to cause GStreamer Good Plugins to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2023-37327)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6269-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6269.1
Version used: `2023-08-03T04:09:35Z`

References
`url: https://ubuntu.com/security/notices/USN-6269-1`
`cve: CVE-2023-37327`
`advisory_id: USN-6269-1`
`cert-bund: WID-SEC-2023-1522`
`dfn-cert: DFN-CERT-2023-3165`
`dfn-cert: DFN-CERT-2023-2941`
`dfn-cert: DFN-CERT-2023-2306`
`dfn-cert: DFN-CERT-2023-2206`
`dfn-cert: DFN-CERT-2023-1813`
`dfn-cert: DFN-CERT-2023-1783`
`dfn-cert: DFN-CERT-2023-1689`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6752-1)

Summary
The remote host is missing an update for the 'freerdp2' package(s) announced via the USN-6752-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libfreerdp2-2
Installed version:    libfreerdp2-2-2.2.0+dfsg1-0ubuntu0.20.04.1
Fixed version:      >=libfreerdp2-2-2.6.1+dfsg1-0ubuntu0.20.04.2
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'freerdp2' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that FreeRDP incorrectly handled certain memory operations. If a user were tricked into connecting to a malicious server, a remote attacker could possibly use this issue to cause FreeRDP to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6752-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6752.1
Version used: `2024-04-26T04:09:00Z`

References
`url: https://ubuntu.com/security/notices/USN-6752-1`
`cve: CVE-2024-32658`
`cve: CVE-2024-32659`
`cve: CVE-2024-32660`
`cve: CVE-2024-32661`
`advisory_id: USN-6752-1`
`cert-bund: WID-SEC-2024-0954`
`dfn-cert: DFN-CERT-2024-1133`
`dfn-cert: DFN-CERT-2024-1106`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6780-1)

Summary
The remote host is missing an update for the 'python-idna' package(s) announced via the USN-6780-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   python3-idna
Installed version:    python3-idna-2.8-1
Fixed version:      >=python3-idna-2.8-1ubuntu0.1
```

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

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'python-idna' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
Guido Vranken discovered that idna did not properly manage certain inputs, which could lead to significant resource consumption. 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-6780-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6780.1
Version used: `2024-05-22T04:08:02Z`

References
`url: https://ubuntu.com/security/notices/USN-6780-1`
`cve: CVE-2024-3651`
`advisory_id: USN-6780-1`
`cert-bund: WID-SEC-2024-1328`
`cert-bund: WID-SEC-2024-1269`
`dfn-cert: DFN-CERT-2024-1433`
`dfn-cert: DFN-CERT-2024-1334`
`dfn-cert: DFN-CERT-2024-0981`

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6719-1)

Summary
The remote host is missing an update for the 'util-linux' package(s) announced via the USN-6719-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   util-linux
Installed version:    util-linux-2.34-0.1ubuntu9.1
Fixed version:      >=util-linux-2.34-0.1ubuntu9.5
```

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
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-6719-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6719.1
Version used: `2024-03-28T04:09:04Z`

References
`url: https://ubuntu.com/security/notices/USN-6719-1`
`cve: CVE-2024-28085`
`advisory_id: USN-6719-1`
`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-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-2
Fixed version:      >=cpio-2.13+dfsg-2ubuntu0.4
```

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-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-2.34-0.1ubuntu9.1
Fixed version:      >=util-linux-2.34-0.1ubuntu9.6
```

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:

... continues on next page ...

... continued from previous page ...

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
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: 4.7)
NVT: Ubuntu: Security Advisory (USN-6319-1)

Summary
The remote host is missing an update for the 'amd64-microcode' package(s) announced via the USN-6319-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   amd64-microcode
Installed version:    amd64-microcode-3.20191218.1ubuntu1
Fixed version:      >=amd64-microcode-3.20191218.1ubuntu1.2
```

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

Affected Software/OS
'amd64-microcode' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
Daniel Trujillo, Johannes Wikner, and Kaveh Razavi discovered that some AMD processors utilising speculative execution and branch prediction may allow unauthorised memory reads via a speculative side-channel attack. A local attacker could use this to expose sensitive information, including kernel memory.

... 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-6319-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6319.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6319-1
cve: CVE-2023-20569
advisory_id: USN-6319-1
cert-bund: WID-SEC-2024-1086
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2023-2011
cert-bund: WID-SEC-2023-2001
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0244
dfn-cert: DFN-CERT-2024-0072
dfn-cert: DFN-CERT-2023-3118
dfn-cert: DFN-CERT-2023-2972
dfn-cert: DFN-CERT-2023-2773
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2580
dfn-cert: DFN-CERT-2023-2508
dfn-cert: DFN-CERT-2023-2390
dfn-cert: DFN-CERT-2023-2389
dfn-cert: DFN-CERT-2023-2385
dfn-cert: DFN-CERT-2023-1968
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1885
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1866
dfn-cert: DFN-CERT-2023-1864
dfn-cert: DFN-CERT-2023-1859
dfn-cert: DFN-CERT-2023-1846
dfn-cert: DFN-CERT-2023-1841
dfn-cert: DFN-CERT-2023-1839
dfn-cert: DFN-CERT-2023-1826

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-1823

Medium (CVSS: 4.7)
NVT: Ubuntu: Security Advisory (USN-5745-1)

Summary
The remote host is missing an update for the 'shadow' package(s) announced via the USN-5745-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   login
Installed version:    login-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=login-1:4.8.1-1ubuntu5.20.04.3
Vulnerable package:   passwd
Installed version:    passwd-1:4.8.1-1ubuntu5.20.04
Fixed version:      >=passwd-1:4.8.1-1ubuntu5.20.04.3
```

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

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

Vulnerability Insight
Florian Weimer discovered that shadow was not properly copying and removing user directory trees, which could lead to a race condition. A local attacker could possibly use this issue to setup a symlink attack and alter or remove directories without authorization.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-5745-1)
OID:1.3.6.1.4.1.25623.1.1.12.2022.5745.1
Version used: 2024-02-02T04:09:01Z

References

```
url: https://ubuntu.com/security/notices/USN-5745-1
cve: CVE-2013-4235
advisory_id: USN-5745-1
dfn-cert: DFN-CERT-2022-2694
```

Medium (CVSS: 4.3)
NVT: Ubuntu: Security Advisory (USN-5286-1)

Summary
The remote host is missing an update for the 'cryptsetup' package(s) announced via the USN-5286-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   cryptsetup
Installed version:    cryptsetup-2:2.2.2-3ubuntu2.3
Fixed version:      >=cryptsetup-2:2.2.2-3ubuntu2.4
```

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

Affected Software/OS
'cryptsetup' package(s) on Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Milan Broz discovered that cryptsetup incorrectly handled LUKS2 reencryption recovery. An attacker with physical access to modify the encrypted device header may trigger the device to be unencrypted the next time it is mounted by the user.
On Ubuntu 20.04 LTS, this issue was fixed by disabling the online reencryption feature.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5286-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5286.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-5286-1
cve: CVE-2021-4122
advisory_id: USN-5286-1
cert-bund: CB-K22/0135
dfn-cert: DFN-CERT-2022-1356
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0089
```

Medium (CVSS: 4.3)
NVT: Ubuntu: Security Advisory (USN-6776-1)

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) announced via the USN-6776-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-5.4.0.77.80
Fixed version:      >=linux-image-generic-5.4.0.182.180
```

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

Affected Software/OS
'linux, linux-aws, linux-aws-5.4, linux-azure, linux-azure-5.4, linux-bluefield, linux-gcp, linux-gcp-5.4, linux-gkeop, linux-hwe-5.4, linux-ibm, linux-ibm-5.4, linux-iot, linux-kvm, linux-oracle, linux-oracle-5.4, linux-raspi, linux-raspi-5.4, linux-xilinx-zynqmp' package(s) on Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
Zheng Wang discovered that the Broadcom FullMAC WLAN driver in the Linux kernel contained a race condition during device removal, leading to a use- after-free vulnerability. A physically proximate attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-47233)
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: - Networking core, - IPv4 networking, - MAC80211 subsystem, - Tomoyo security module, (CVE-2024-26614, CVE-2023-52530, CVE-2024-26622)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6776-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6776.1
Version used: `2024-05-17T04:08:09Z`

References

```
url: https://ubuntu.com/security/notices/USN-6776-1
cve: CVE-2023-47233
cve: CVE-2023-52530
cve: CVE-2024-26614
cve: CVE-2024-26622
advisory_id: USN-6776-1
cert-bund: WID-SEC-2024-0536
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2024-0527
cert-bund: WID-SEC-2023-2828
dfn-cert: DFN-CERT-2024-1552
dfn-cert: DFN-CERT-2024-1542
dfn-cert: DFN-CERT-2024-1518
dfn-cert: DFN-CERT-2024-1508
dfn-cert: DFN-CERT-2024-1492
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1351
dfn-cert: DFN-CERT-2024-1338
dfn-cert: DFN-CERT-2024-1337
dfn-cert: DFN-CERT-2024-1336
dfn-cert: DFN-CERT-2024-1333
dfn-cert: DFN-CERT-2024-1327
dfn-cert: DFN-CERT-2024-1249
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1077
dfn-cert: DFN-CERT-2024-1058
dfn-cert: DFN-CERT-2024-1057
dfn-cert: DFN-CERT-2024-1056
dfn-cert: DFN-CERT-2024-1055
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-0986
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-2024-0614
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
```

[return to 192.168.218.129]

2.1.4 Medium general/tcp

Medium (CVSS: 6.8)
NVT: Wireshark < 4.2.0 DoS Vulnerabilities

Product detection result
cpe:/a:wireshark:wireshark:3.2.3
Detected by Wireshark Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1
↪.0.800039)

Summary
Wireshark is prone to multiple denial of service (DoS) vulnerabilities.

Quality of Detection: 97

Vulnerability Detection Result
Installed version: 3.2.3
Fixed version: 4.2.0
Installation
path / port: /usr/bin/wireshark

Impact
Successful exploitation may allow remote attackers to perform denial of service on an affected system.

Solution:
Solution type: VendorFix
Update to version 4.2.0 or later.

Affected Software/OS
Wireshark versions prior to 4.2.0.

Vulnerability Insight
Multiple flaws exist due to:
- An issue in Wireshark function dissect_bgp_open of file packet-bgp.c.
- A buffer overflow vulnerability in ws_manuf_lookup_str of file pan/addr_resolv.c.
- A buffer overflow vulnerability in format_fractional_part_nsecs of file wsutil/to_str.c.
For more information about the vulnerabilities refer to Reference links.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Wireshark < 4.2.0 DoS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.128009
Version used: 2024-04-23T05:05:27Z

Product Detection Result
Product: cpe:/a:wireshark:wireshark:3.2.3
Method: Wireshark Detection (Linux/Unix SSH Login)

. . . continues on next page . . .

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.800039)

References

cve: CVE-2024-24478
cve: CVE-2024-24476
cve: CVE-2024-24479
url: https://gist.github.com/1047524396/e82c55147cd3cb62ef20cbdb0ec83694
url: https://gist.github.com/1047524396/369ba0ccffe255cf8142208b6142be2b
url: https://gist.github.com/1047524396/c50ad17e9a1a18990043a7cd27814c78
cert-bund: WID-SEC-2024-0455
cert-bund: WID-SEC-2024-0448
dfn-cert: DFN-CERT-2024-1046

Medium (CVSS: 6.5)
NVT: Missing Linux Kernel mitigations for 'RETbleed' hardware vulnerabilities (INTEL-SA-00702, AMD-SB-1037)

Summary

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

Quality of Detection: 80

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                                | Linux Kernel status (SSH resp
↪onse)
-------------------------------------------------------------------------------
↪-----------------------------------------------------------------------
/sys/devices/system/cpu/vulnerabilities/retbleed | sysfs file missing (cat: /sys
↪/devices/system/cpu/vulnerabilities/retbleed: No such file or directory)
Notes on the "Linux 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 current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system 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
The following solutions exist:

... continues on next page ...

... continued from previous page ...

- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)
Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard
Note: Please create an override for this result if one of the following applies:
- the sysfs file is not available but other mitigations like a Microcode update is already in place
- the sysfs file is not available but the CPU of the host is not affected
- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)

Affected Software/OS
Various Intel and AMD CPUs. Please see the references for the full list of affected CPUs.

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 (INTEL.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.104601
Version used: `2024-06-14T05:05:48Z`

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/security-center/advisory/intel-sa-0`
`↪0702.html`
`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`
`url: https://www.intel.com/content/www/us/en/developer/topic-technology/software`
`↪-security-guidance/processors-affected-consolidated-product-cpu-model.html`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-1737`
`cert-bund: WID-SEC-2022-0665`
`cert-bund: WID-SEC-2022-0659`
`cert-bund: WID-SEC-2022-0650`
`dfn-cert: DFN-CERT-2024-1554`
`dfn-cert: DFN-CERT-2024-0371`
`dfn-cert: DFN-CERT-2024-0370`
`dfn-cert: DFN-CERT-2023-1595`
`dfn-cert: DFN-CERT-2023-0863`
`dfn-cert: DFN-CERT-2023-0376`
`dfn-cert: DFN-CERT-2022-2919`
`dfn-cert: DFN-CERT-2022-2914`
`dfn-cert: DFN-CERT-2022-2858`

... continues on next page ...

... continued from previous page ...

```
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: 6.5)
NVT: Wireshark Security Update (wnpa-sec-2020-10) - Linux

Product detection result

```
cpe:/a:wireshark:wireshark:3.2.3
Detected by Wireshark Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25623.1
↪.0.800039)
```

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

```
Installed version: 3.2.3
Fixed version:     3.2.6
Installation
path / port:       /usr/bin/wireshark
```

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation would allow an attacker to crash the application.

Solution:
Solution type: VendorFix
Update to version 3.2.6.

Affected Software/OS
Wireshark version 3.2.0 through 3.2.5.

Vulnerability Insight
The vulnerability exists because of a double free during LZ4 decompression in epan/dissectors/packet-kafka.c.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Wireshark Security Update (wnpa-sec-2020-10) - Linux`
OID:1.3.6.1.4.1.25623.1.0.113744
Version used: `2021-07-06T11:00:47Z`

Product Detection Result
Product: `cpe:/a:wireshark:wireshark:3.2.3`
Method: `Wireshark Detection (Linux/Unix SSH Login)`
OID: 1.3.6.1.4.1.25623.1.0.800039)

References
`cve: CVE-2020-17498`
`url: https://www.wireshark.org/security/wnpa-sec-2020-10.html`
`url: https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=76afda9`
`↪63de4f0b9be24f2d8e873990a5cbf221b`
`cert-bund: WID-SEC-2023-1918`
`cert-bund: CB-K20/0820`
`dfn-cert: DFN-CERT-2023-1743`
`dfn-cert: DFN-CERT-2020-2006`
`dfn-cert: DFN-CERT-2020-1796`

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

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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "spec_stor
↪e_bypass" hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                          | Linux Kernel status
↪(SSH response)
-------------------------------------------------------------------------------
↪--------------
/sys/devices/system/cpu/vulnerabilities/spec_store_bypass | Vulnerable
Notes on the "Linux 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 current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system 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
The following solutions exist:
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)
Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard
Note: Please create an override for this result if one of the following applies:
- the sysfs file is not available but other mitigations like a Microcode update is already in place
- the sysfs file is not available but the CPU of the host is not affected
- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)

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: `2024-06-14T05:05:48Z`

References

```
cve: CVE-2018-3639
url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/index.html
url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-0
↪0115.html
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2072
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-2023-1947
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2302
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1767
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1658
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
```

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 4.7)
NVT: Missing Linux Kernel mitigations for 'Speculative Return Stack Overflow (SRSO)' hardware vulnerability (INCEPTION, AMD-SB-7005)

Summary
The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Speculative Return Stack Overflow (SRSO)' hardware vulnerability dubbed 'INCEPTION'.

Quality of Detection: 80

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "spec_rsta
↪ck_overflow" hardware vulnerability as reported by the sysfs interface:
sysfs file checked                                          | Linux Kernel stat
↪us (SSH response)
--------------------------------------------------------------------------------
```

... continues on next page ...

... continued from previous page ...

```
↪--------------------------------------------------------------------------------
↪-----------------
/sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow | sysfs file missin
↪g (cat: /sys/devices/system/cpu/vulnerabilities/spec_rstack_overflow: No such
↪file or directory)
Notes on the "Linux 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 current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system 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
The following solutions exist:
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)
Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard
Note: Please create an override for this result if one of the following applies:
- the sysfs file is not available but other mitigations like a Microcode update is already in place
- the sysfs file is not available but the CPU of the host is not affected
- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)

Affected Software/OS
Various AMD CPUs. Please see the references for the full list of affected CPUs.

Vulnerability Detection Method
Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'Speculative Return Stack Overflow (SRSO)'.
↪..`
OID:1.3.6.1.4.1.25623.1.0.104897
Version used: `2024-06-14T05:05:48Z`

References
`cve: CVE-2023-20569`
`url: https://docs.kernel.org/admin-guide/hw-vuln/srso.html`
`url: https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html`
`url: https://comsec.ethz.ch/research/microarch/inception/`
`cert-bund: WID-SEC-2024-1086`
`cert-bund: WID-SEC-2024-0064`
`cert-bund: WID-SEC-2023-2011`

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-2001
dfn-cert: DFN-CERT-2024-0333
dfn-cert: DFN-CERT-2024-0250
dfn-cert: DFN-CERT-2024-0244
dfn-cert: DFN-CERT-2024-0072
dfn-cert: DFN-CERT-2023-3118
dfn-cert: DFN-CERT-2023-2972
dfn-cert: DFN-CERT-2023-2773
dfn-cert: DFN-CERT-2023-2687
dfn-cert: DFN-CERT-2023-2580
dfn-cert: DFN-CERT-2023-2508
dfn-cert: DFN-CERT-2023-2390
dfn-cert: DFN-CERT-2023-2389
dfn-cert: DFN-CERT-2023-2385
dfn-cert: DFN-CERT-2023-1968
dfn-cert: DFN-CERT-2023-1966
dfn-cert: DFN-CERT-2023-1965
dfn-cert: DFN-CERT-2023-1964
dfn-cert: DFN-CERT-2023-1949
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2023-1889
dfn-cert: DFN-CERT-2023-1886
dfn-cert: DFN-CERT-2023-1885
dfn-cert: DFN-CERT-2023-1884
dfn-cert: DFN-CERT-2023-1878
dfn-cert: DFN-CERT-2023-1866
dfn-cert: DFN-CERT-2023-1864
dfn-cert: DFN-CERT-2023-1859
dfn-cert: DFN-CERT-2023-1846
dfn-cert: DFN-CERT-2023-1841
dfn-cert: DFN-CERT-2023-1839
dfn-cert: DFN-CERT-2023-1826
dfn-cert: DFN-CERT-2023-1823
```

[return to 192.168.218.129]

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.

... continues on next page ...

... continued from previous page ...

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
- 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 192.168.218.129]

2.1.6 Low package

Low (CVSS: 3.9)
NVT: Ubuntu: Security Advisory (USN-6257-1)

Summary
The remote host is missing an update for the 'open-vm-tools' package(s) announced via the USN-6257-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   open-vm-tools
Installed version:    open-vm-tools-2:11.2.5-2ubuntu1~ubuntu20.04.1
Fixed version:      >=open-vm-tools-2:11.3.0-2ubuntu0~ubuntu20.04.5
```

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

Affected Software/OS
'open-vm-tools' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04.

Vulnerability Insight
It was discovered that Open VM Tools incorrectly handled certain authentication requests. A fully compromised ESXi host can force Open VM Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. (CVE-2023-20867)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6257-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6257.1
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6257-1
cve: CVE-2023-20867
advisory_id: USN-6257-1
cert-bund: WID-SEC-2023-2625
cert-bund: WID-SEC-2023-1456
dfn-cert: DFN-CERT-2023-2039
dfn-cert: DFN-CERT-2023-1366
```

Low (CVSS: 3.7)
NVT: Ubuntu: Security Advisory (USN-6811-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'openjdk-lts' package(s) announced via the USN-6811-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   openjdk-11-jre
Installed version:    openjdk-11-jre-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-11.0.23+9-1ubuntu1~20.04.2
Vulnerable package:   openjdk-11-jre-headless
Installed version:    openjdk-11-jre-headless-11.0.11+9-0ubuntu2~20.04
Fixed version:      >=openjdk-11-jre-headless-11.0.23+9-1ubuntu1~20.04.2
```

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

Affected Software/OS
'openjdk-lts' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that the Hotspot component of OpenJDK 11 incorrectly handled certain exceptions with specially crafted long messages. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-21011)
It was discovered that OpenJDK 11 incorrectly performed reverse DNS query under certain circumstances in the Networking/HTTP client component. An attacker could possibly use this issue to obtain sensitive information. (CVE-2024-21012)
Vladimir Kondratyev discovered that the Hotspot component of OpenJDK 11 incorrectly handled address offset calculations in the C1 compiler. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-21068)
Yakov Shafranovich discovered that OpenJDK 11 did not properly manage memory in the Pack200 archive format. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-21085)
It was discovered that the Hotspot component of OpenJDK 11 incorrectly handled array accesses in the C2 compiler. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-21094)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6811-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6811.1
Version used: `2024-06-07T04:08:49Z`

References
`url: https://ubuntu.com/security/notices/USN-6811-1`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2024-21011
cve: CVE-2024-21012
cve: CVE-2024-21068
cve: CVE-2024-21085
cve: CVE-2024-21094
advisory_id: USN-6811-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1272
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
```

Low (CVSS: 3.7)
NVT: Ubuntu: Security Advisory (USN-5587-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5587-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.68.0-1ubuntu2.5
Fixed version:      >=curl-7.68.0-1ubuntu2.13
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl3-gnutls-7.68.0-1ubuntu2.13
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.68.0-1ubuntu2.5
Fixed version:      >=libcurl4-7.68.0-1ubuntu2.13
```

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

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

Axel Chong discovered that when curl accepted and sent back cookies containing control bytes that a HTTP(S) server might return a 400 (Bad Request Error) response. A malicious cookie host could possibly use this to cause denial-of-service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5587-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5587.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5587-1`
`cve: CVE-2022-35252`
`advisory_id: USN-5587-1`
`cert-bund: WID-SEC-2024-0794`
`cert-bund: WID-SEC-2023-2229`
`cert-bund: WID-SEC-2023-1728`
`cert-bund: WID-SEC-2023-1614`
`cert-bund: WID-SEC-2023-1424`
`cert-bund: WID-SEC-2023-1350`
`cert-bund: WID-SEC-2023-0296`
`cert-bund: WID-SEC-2023-0189`
`cert-bund: WID-SEC-2022-2372`
`cert-bund: WID-SEC-2022-1231`
`dfn-cert: DFN-CERT-2024-0230`
`dfn-cert: DFN-CERT-2023-1423`
`dfn-cert: DFN-CERT-2023-1044`
`dfn-cert: DFN-CERT-2023-0372`
`dfn-cert: DFN-CERT-2023-0278`
`dfn-cert: DFN-CERT-2023-0214`
`dfn-cert: DFN-CERT-2023-0158`
`dfn-cert: DFN-CERT-2023-0157`
`dfn-cert: DFN-CERT-2022-2799`
`dfn-cert: DFN-CERT-2022-2400`
`dfn-cert: DFN-CERT-2022-1910`

Low (CVSS: 3.7)
NVT: Ubuntu: Security Advisory (USN-6810-1)

Summary
The remote host is missing an update for the 'openjdk-8' package(s) announced via the USN-6810-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Vulnerable package:   openjdk-8-jdk
Installed version:    openjdk-8-jdk-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-8u412-ga-1~20.04.1
Vulnerable package:   openjdk-8-jdk-headless
Installed version:    openjdk-8-jdk-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jdk-headless-8u412-ga-1~20.04.1
Vulnerable package:   openjdk-8-jre
Installed version:    openjdk-8-jre-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-8u412-ga-1~20.04.1
Vulnerable package:   openjdk-8-jre-headless
Installed version:    openjdk-8-jre-headless-8u292-b10-0ubuntu1~20.04
Fixed version:      >=openjdk-8-jre-headless-8u412-ga-1~20.04.1
```

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

Affected Software/OS
'openjdk-8' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10, Ubuntu 24.04.

Vulnerability Insight
It was discovered that the Hotspot component of OpenJDK 8 incorrectly handled certain exceptions with specially crafted long messages. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-21011)
Vladimir Kondratyev discovered that the Hotspot component of OpenJDK 8 incorrectly handled address offset calculations in the C1 compiler. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-21068)
Yakov Shafranovich discovered that OpenJDK 8 did not properly manage memory in the Pack200 archive format. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-21085)
It was discovered that the Hotspot component of OpenJDK 8 incorrectly handled array accesses in the C2 compiler. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2024-21094)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6810-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6810.1
Version used: `2024-06-07T04:08:49Z`

References
`url: https://ubuntu.com/security/notices/USN-6810-1`
`cve: CVE-2024-21011`
`cve: CVE-2024-21068`
`cve: CVE-2024-21085`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2024-21094
advisory_id: USN-6810-1
cert-bund: WID-SEC-2024-1248
cert-bund: WID-SEC-2024-1226
cert-bund: WID-SEC-2024-0895
dfn-cert: DFN-CERT-2024-1436
dfn-cert: DFN-CERT-2024-1272
dfn-cert: DFN-CERT-2024-1251
dfn-cert: DFN-CERT-2024-1032
dfn-cert: DFN-CERT-2024-1005
dfn-cert: DFN-CERT-2024-1004
```

Low (CVSS: 3.3)
NVT: Ubuntu: Security Advisory (USN-5391-1)

Summary
The remote host is missing an update for the 'libsepol' package(s) announced via the USN-5391-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result

```
Vulnerable package:   libsepol1
Installed version:    libsepol1-3.0-1
Fixed version:      >=libsepol1-3.0-1ubuntu0.1
```

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

Affected Software/OS
'libsepol' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 21.10.

Vulnerability Insight
Nicolas Iooss discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36084)
It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36085)
It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affects Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2021-36086)

... continues on next page ...

. . . continued from previous page . . .

It was discovered that libsepol incorrectly validated certain data, leading to a heap overflow. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36087)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5391-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5391.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-5391-1`
`cve: CVE-2021-36084`
`cve: CVE-2021-36085`
`cve: CVE-2021-36086`
`cve: CVE-2021-36087`
`advisory_id: USN-5391-1`
`cert-bund: WID-SEC-2022-0571`
`cert-bund: CB-K21/1164`
`dfn-cert: DFN-CERT-2021-2527`
`dfn-cert: DFN-CERT-2021-2374`

Low (CVSS: 3.3)
NVT: Ubuntu: Security Advisory (USN-6477-1)

Summary
The remote host is missing an update for the 'procps' package(s) announced via the USN-6477-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   procps
Installed version:    procps-2:3.3.16-1ubuntu2.2
Fixed version:      >=procps-2:3.3.16-1ubuntu2.4
```

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

Affected Software/OS
'procps' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

It was discovered that the procps-ng ps tool incorrectly handled memory. An attacker could possibly use this issue to cause procps-ng to crash, resulting in a denial of service.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6477-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6477.1
Version used: `2024-02-02T04:09:01Z`

References
`url: https://ubuntu.com/security/notices/USN-6477-1`
`cve: CVE-2023-4016`
`advisory_id: USN-6477-1`
`cert-bund: WID-SEC-2024-0869`
`cert-bund: WID-SEC-2023-3146`
`cert-bund: WID-SEC-2023-2853`
`dfn-cert: DFN-CERT-2023-1894`

Low (CVSS: 3.3)
NVT: Ubuntu: Security Advisory (USN-6687-1)

Summary
The remote host is missing an update for the 'accountsservice' package(s) announced via the USN-6687-1 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   accountsservice
Installed version:    accountsservice-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=accountsservice-0.6.55-0ubuntu12~20.04.7
Vulnerable package:   libaccountsservice0
Installed version:    libaccountsservice0-0.6.55-0ubuntu12~20.04.4
Fixed version:      >=libaccountsservice0-0.6.55-0ubuntu12~20.04.7
```

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

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

Vulnerability Insight
It was discovered that AccountsService called a helper incorrectly when performing password change operations. A local attacker could possibly use this issue to obtain encrypted passwords.

... 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-6687-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6687.1
Version used: `2024-03-12T04:09:07Z`

References
`url: https://ubuntu.com/security/notices/USN-6687-1`
`cve: CVE-2012-6655`
`advisory_id: USN-6687-1`
`dfn-cert: DFN-CERT-2024-0651`

[return to 192.168.218.129]

2.1.7 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
`cpe:/a:ssh:ssh2`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↪)`

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

Quality of Detection: 80

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).

... continues on next page ...

... continued from previous page ...

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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ssh:ssh2`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

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

[return to 192.168.218.129]

2.1.8 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: 735994820
Packet 2: 735995878
```

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

Solution:
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

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 192.168.218.129]