Scan Report

July 1, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scan MISP". The scan started at Sun Jun 19 13:24:19 2022 UTC and ended at Sun Jun 19 13:28:52 2022 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
192.168.2.3	10	3	0	0	0
Total: 1	10	3	0	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 13 results selected by the filtering described above. Before filtering there were 270 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.2.3	SSH	Success	Protocol SSH, Port 22, User misp

2 Results per Host

2.1 192.168.2.3

Host scan start	Sun Jun 19 13:25:16 2022 UTC
Host scan end	Sun Jun 19 13:28:50 2022 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium

2.1.1 High general/tcp

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

. . . continues on next page . . .

... continued from previous page ...

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

Vulnerability Detection Result

```
Vulnerable package: libavcodec57
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
Vulnerable package: libavformat57
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
Vulnerable package: libavresample3
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
Vulnerable package: libavutil55
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
Vulnerable package: libswresample2
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
Vulnerable package: libswscale4
Installed version:  3.4.8-0ubuntu0.2
Fixed version:      7:3.4.11-0ubuntu0.1
```

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

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

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 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. (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)

... continues on next page ...

... continued from previous page ...

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, Ubuntu 20.04 LTS and Ubuntu 21.10. (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)
It was discovered that FFm ...
Description truncated. Please see the references for more information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory for ffmpeg (USN-5472-1)`
OID:1.3.6.1.4.1.25623.1.0.845409
Version used: `2022-06-15T14:04:03Z`

References
`cve: CVE-2020-20445`
`cve: CVE-2020-20446`
`cve: CVE-2020-20453`
`cve: CVE-2020-20450`
`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-2020-22020`
`cve: CVE-2020-22022`
`cve: CVE-2020-22023`
`cve: CVE-2022-22025`
`cve: CVE-2020-22026`
`cve: CVE-2020-22028`
`cve: CVE-2020-22031`
`cve: CVE-2020-22032`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2020-22034
cve: CVE-2020-22036
cve: CVE-2020-22042
cve: CVE-2020-22019
cve: CVE-2020-22021
cve: CVE-2020-22033
cve: CVE-2020-22027
cve: CVE-2020-22029
cve: CVE-2020-22030
cve: CVE-2020-22035
cve: CVE-2020-22037
cve: CVE-2020-35965
cve: CVE-2021-38114
cve: CVE-2021-38171
cve: CVE-2022-1475
cve: CVE-2020-22025
cve: CVE-2021-38291
advisory-id: USN-5472-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006623
↪.html
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-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 for ntfs-3g (USN-5463-1)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5463-1 advisory.

Vulnerability Detection Result
`Vulnerable package: ntfs-3g`
`Installed version: 2017.3.23-2ubuntu0.18.04.3`
`Fixed version: 1:2017.3.23-2ubuntu0.18.04.4`

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 22.04 LTS, Ubuntu 21.10, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS.

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 for ntfs-3g (USN-5463-1)`
OID:1.3.6.1.4.1.25623.1.0.845400
Version used: `2022-06-15T14:04:03Z`

References
`cve: CVE-2021-46790`
`cve: CVE-2022-30783`
`cve: CVE-2022-30784`
`cve: CVE-2022-30786`
`cve: CVE-2022-30788`
`cve: CVE-2022-30789`

. . . continues on next page . . .

... continued from previous page ...

cve: CVE-2022-30785
cve: CVE-2022-30787
advisory-id: USN-5463-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006611
↪.html
dfn-cert: DFN-CERT-2022-1218
dfn-cert: DFN-CERT-2022-1217

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

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

Vulnerability Detection Result
Vulnerable package: dpkg
Installed version: 1.19.0.5ubuntu2.3
Fixed version: 1.19.0.5ubuntu2.4
Vulnerable package: libdpkg-perl
Installed version: 1.19.0.5ubuntu2.3
Fixed version: 1.19.0.5ubuntu2.4

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

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

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 for dpkg (USN-5446-1)
OID:1.3.6.1.4.1.25623.1.0.845385
Version used: 2022-06-09T03:04:58Z

References
cve: CVE-2022-1664
advisory-id: USN-5446-1

... continues on next page ...

... continued from previous page ...

url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006586.html
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1194

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory for linux (USN-5418-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-5418-1 advisory.

Vulnerability Detection Result
Vulnerable package: linux-image-generic
Installed version: 4.15.0.176.165
Fixed version: 4.15.0.177.166

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

Affected Software/OS
'linux' package(s) on Ubuntu 18.04 LTS.

Vulnerability Insight
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)
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-2022-23042)
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 execute arbitrary code. (CVE-2022-24958)
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)
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)

... continues on next page ...

... continued from previous page ...

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 USB SR9700 ethernet device driver for the Linux kernel did not properly validate the length of requests from the device. A physically proximate attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2022-26966)
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 for linux (USN-5418-1)`
OID:1.3.6.1.4.1.25623.1.0.845369
Version used: `2022-05-23T14:06:16Z`

References
`cve: CVE-2021-26401`
`cve: CVE-2022-23036`
`cve: CVE-2022-23037`
`cve: CVE-2022-23038`
`cve: CVE-2022-23039`
`cve: CVE-2022-23040`
`cve: CVE-2022-23042`
`cve: CVE-2022-24958`
`cve: CVE-2022-25258`
`cve: CVE-2022-25375`
`cve: CVE-2022-26490`
`cve: CVE-2022-26966`
`cve: CVE-2022-27223`
`advisory-id: USN-5418-1`
`url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006559.`
`↪html`
`cert-bund: CB-K22/0686`
`cert-bund: CB-K22/0379`
`cert-bund: CB-K22/0309`
`cert-bund: CB-K22/0300`
`cert-bund: CB-K22/0281`
`cert-bund: CB-K22/0215`
`cert-bund: CB-K22/0202`
`cert-bund: CB-K22/0177`
`dfn-cert: DFN-CERT-2022-1294`
`dfn-cert: DFN-CERT-2022-1280`
`dfn-cert: DFN-CERT-2022-1277`
`dfn-cert: DFN-CERT-2022-1256`
`dfn-cert: DFN-CERT-2022-1082`

... continues on next page ...

... continued from previous page ...

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-2022-0991
dfn-cert: DFN-CERT-2022-0976
dfn-cert: DFN-CERT-2022-0930
dfn-cert: DFN-CERT-2022-0921
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0893
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-2022-0819
dfn-cert: DFN-CERT-2022-0803
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-2022-0676
dfn-cert: DFN-CERT-2022-0663
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-2022-0547
dfn-cert: DFN-CERT-2022-0543
dfn-cert: DFN-CERT-2022-0541
dfn-cert: DFN-CERT-2022-0539
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

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory for imagemagick (USN-5456-1)

Summary
The remote host is missing an update for the 'imagemagick' package(s) announced via the USN-5456-1 advisory.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
Vulnerable package: imagemagick
Installed version:  6.9.7.4+dfsg-16ubuntu6.12
Fixed version:      8:6.9.7.4+dfsg-16ubuntu6.13
Vulnerable package: imagemagick-6-common
Installed version:  6.9.7.4+dfsg-16ubuntu6.12
Fixed version:      8:6.9.7.4+dfsg-16ubuntu6.13
Vulnerable package: libmagickcore-6.q16-3
Installed version:  6.9.7.4+dfsg-16ubuntu6.12
Fixed version:      8:6.9.7.4+dfsg-16ubuntu6.13
```

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

Affected Software/OS
'imagemagick' package(s) on Ubuntu 18.04 LTS.

Vulnerability Insight
It was discovered that ImageMagick incorrectly handled memory under certain circumstances. If a user were tricked into opening a specially crafted image, an attacker could possibly exploit this issue to cause a denial of service or other unspecified impact.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory for imagemagick (USN-5456-1)`
OID:1.3.6.1.4.1.25623.1.0.845395
Version used: `2022-06-15T14:04:03Z`

References

```
cve: CVE-2022-28463
advisory-id: USN-5456-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006603
↪.html
cert-bund: CB-K22/0548
dfn-cert: DFN-CERT-2022-1228
dfn-cert: DFN-CERT-2022-1158
dfn-cert: DFN-CERT-2022-1104
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory for e2fsprogs (USN-5464-1)

Summary

... continues on next page ...

... continued from previous page ...

The remote host is missing an update for the 'e2fsprogs' package(s) announced via the USN-5464-1 advisory.

Vulnerability Detection Result

```
Vulnerable package: e2fsprogs
Installed version:  1.44.1-1ubuntu1.3
Fixed version:      1.44.1-1ubuntu1.4
```

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

Affected Software/OS
'e2fsprogs' package(s) on Ubuntu 22.04 LTS, Ubuntu 21.10, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS.

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 for e2fsprogs (USN-5464-1)`
OID:1.3.6.1.4.1.25623.1.0.845399
Version used: `2022-06-15T14:04:03Z`

References

```
cve: CVE-2022-1304
advisory-id: USN-5464-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006612
↪.html
cert-bund: CB-K22/0616
dfn-cert: DFN-CERT-2022-1091
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory for nss (USN-5410-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5410-1 advisory.

Vulnerability Detection Result

```
Vulnerable package: libnss3
Installed version:  3.35-2ubuntu2.13
Fixed version:      2:3.35-2ubuntu2.14
```

... continues on next page ...

... continued from previous page ...

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

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

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 for nss (USN-5410-1)`
OID:1.3.6.1.4.1.25623.1.0.845364
Version used: `2022-05-23T14:06:16Z`

References
```
cve: CVE-2020-25648
advisory-id: USN-5410-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006552.
↪html
cert-bund: CB-K21/1095
cert-bund: CB-K21/0466
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 for gnupg2 (USN-5431-1)

Summary
The remote host is missing an update for the 'gnupg2' package(s) announced via the USN-5431-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: gnupg
Installed version:  2.2.4-1ubuntu1.4
Fixed version:      2.2.4-1ubuntu1.5
```

Solution:

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
'gnupg2' package(s) on Ubuntu 18.04 LTS.

Vulnerability Insight
It was discovered that GnuPG was not properly processing keys with large amounts of signatures. 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 for gnupg2 (USN-5431-1)`
OID:1.3.6.1.4.1.25623.1.0.845389
Version used: `2022-06-02T06:55:59Z`

References
`cve: CVE-2019-13050`
`advisory-id: USN-5431-1`
`url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006592.html`
`cert-bund: CB-K20/1072`
`dfn-cert: DFN-CERT-2021-1070`
`dfn-cert: DFN-CERT-2021-0107`
`dfn-cert: DFN-CERT-2019-1430`

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory for curl (USN-5412-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5412-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: curl
Installed version:  7.58.0-2ubuntu3.17
Fixed version:      7.58.0-2ubuntu3.18
Vulnerable package: libcurl3-gnutls
Installed version:  7.58.0-2ubuntu3.17
Fixed version:      7.58.0-2ubuntu3.18
Vulnerable package: libcurl4
Installed version:  7.58.0-2ubuntu3.17
Fixed version:      7.58.0-2ubuntu3.18
```

Solution:

... continues on next page ...

... continued from previous page ...

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

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

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.
Details: `Ubuntu: Security Advisory for curl (USN-5412-1)`
OID:1.3.6.1.4.1.25623.1.0.845363
Version used: `2022-06-16T03:04:08Z`

References
```
cve: CVE-2022-27780
cve: CVE-2022-27781
cve: CVE-2022-27782
advisory-id: USN-5412-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006553.
↪html
cert-bund: CB-K22/0570
dfn-cert: DFN-CERT-2022-1140
dfn-cert: DFN-CERT-2022-1049
```

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory for tiff (USN-5421-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5421-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: libtiff5
Installed version:  4.0.9-5ubuntu0.4
Fixed version:      4.0.9-5ubuntu0.5
```

... continues on next page ...

... continued from previous page ...

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

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

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 for tiff (USN-5421-1)`
OID:1.3.6.1.4.1.25623.1.0.845371
Version used: `2022-05-23T14:06:16Z`

References
`cve: CVE-2020-35522`
`cve: CVE-2022-0561`
`cve: CVE-2022-0562`
`cve: CVE-2022-0891`
`cve: CVE-2022-0865`
`advisory-id: USN-5421-1`
`url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006562.html`
`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`

[return to 192.168.2.3]

2.1.2 Medium general/tcp

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory for cron (USN-5259-3)

Summary
The remote host is missing an update for the 'cron' package(s) announced via the USN-5259-3 advisory.

Vulnerability Detection Result
`Vulnerable package: cron`
`Installed version: 3.0pl1-128.1ubuntu1.1`
`Fixed version: 3.0pl1-128.1ubuntu1.2`

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

Affected Software/OS
'cron' package(s) on Ubuntu 18.04 LTS.

Vulnerability Insight
USN-5259-1 and USN-5259-2 fixed vulnerabilities in Cron. 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 the postinst maintainer script in Cron unsafely handled file permissions during package install or update operations. An attacker could possibly use this issue to perform a privilege escalation attack. (CVE-2017-9525) Florian Weimer discovered that Cron incorrectly handled certain memory operations during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9704) It was discovered that Cron incorrectly handled user input during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9705) It was discovered that Cron contained a use-after-free vulnerability in its force_rescan_user function. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9706)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory for cron (USN-5259-3)`
OID:1.3.6.1.4.1.25623.1.0.845362
Version used: `2022-05-23T14:06:16Z`

References
`cve: CVE-2017-9525`
`cve: CVE-2019-9704`
`cve: CVE-2019-9705`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2019-9706
advisory-id: USN-5259-3
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-May/006551.
↪html
dfn-cert: DFN-CERT-2019-0575
dfn-cert: DFN-CERT-2019-0540
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory for linux (USN-5466-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-5466-1 advisory.

Vulnerability Detection Result
`Vulnerable package: linux-image-generic`
`Installed version: 4.15.0.176.165`
`Fixed version: 4.15.0.184.172`

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

Affected Software/OS
'linux' package(s) on Ubuntu 18.04 LTS.

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)
It was discovered that the btrfs file system implementation in the Linux kernel did not properly handle locking in certain error conditions. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2021-4149)
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 virtual graphics memory manager implementation in the Linux kernel was subject to a race condition, potentially leading to an information leak. (CVE-2022-1419)

... continues on next page ...

... continued from previous page ...

discovered that the 802.2 LLC type 2 driver in the Linux kernel did not properly perform reference counting in some error conditions. A local attacker could use this to cause a denial of service. (CVE-2022-28356)
It was discovered that the EMS CAN/USB interface implementation in the Linux kernel contained a double-free vulnerability when handling certain error conditions. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2022-28390)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory for linux (USN-5466-1)`
OID:1.3.6.1.4.1.25623.1.0.845407
Version used: `2022-06-15T14:04:03Z`

References
`cve: CVE-2022-21499`
`cve: CVE-2022-1966`
`cve: CVE-2021-3772`
`cve: CVE-2021-4149`
`cve: CVE-2022-1016`
`cve: CVE-2022-1419`
`cve: CVE-2022-28356`
`cve: CVE-2022-28390`
`advisory-id: USN-5466-1`
`url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006614`
`↪.html`
`cert-bund: CB-K22/0672`
`cert-bund: CB-K22/0651`
`cert-bund: CB-K22/0607`
`cert-bund: CB-K22/0437`
`cert-bund: CB-K22/0361`
`cert-bund: CB-K22/0347`
`cert-bund: CB-K22/0260`
`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-2022-1244`
`dfn-cert: DFN-CERT-2022-1182`
`dfn-cert: DFN-CERT-2022-1181`
`dfn-cert: DFN-CERT-2022-1110`
`dfn-cert: DFN-CERT-2022-1092`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1082
dfn-cert: DFN-CERT-2022-1075
dfn-cert: DFN-CERT-2022-1072
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-2022-0930
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0915
dfn-cert: DFN-CERT-2022-0895
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-2022-0790
dfn-cert: DFN-CERT-2022-0783
dfn-cert: DFN-CERT-2022-0766
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0439
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-2022-0260
dfn-cert: DFN-CERT-2022-0251
dfn-cert: DFN-CERT-2022-0196
dfn-cert: DFN-CERT-2022-0186
dfn-cert: DFN-CERT-2022-0092
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

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory for ca-certificates (USN-5473-1)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5473-1 advisory.

Vulnerability Detection Result
Vulnerable package: ca-certificates
Installed version: 20210119~18.04.2
Fixed version: 20211016~18.04.1

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 21.10, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS.

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 for ca-certificates (USN-5473-1)
OID:1.3.6.1.4.1.25623.1.0.845405
Version used: 2022-06-15T04:37:18Z

References
advisory-id: USN-5473-1
url: https://lists.ubuntu.com/archives/ubuntu-security-announce/2022-June/006620
↪.html

[return to 192.168.2.3]

This file was automatically generated.