Scan Report

July 20, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “RACE- Data”. The scan started at Wed Jul 19 23:59:14 2023 UTC and ended at Thu Jul 20 00:26:46 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.10 ip-10-0-0-10.us-east-2.compute.internal	273	134	5	0	0
Total: 1	273	134	5	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 excluded from the report.
Notes are excluded from 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 412 results selected by the filtering described above. Before filtering there were 1314 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.10 - ip-10-0-0-10.us-east-2.compute.internal	SSH	Success	Protocol SSH, Port 22, User vagrant
10.0.0.10 - ip-10-0-0-10.us-east-2.compute.internal	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.0.0.10

Host scan start	Wed Jul 19 23:59:55 2023 UTC
Host scan end	Thu Jul 20 00:26:39 2023 UTC

Service (Port)	Threat Level
general/tcp	High
80/tcp	High
package	High
631/tcp	High
22/tcp	High
21/tcp	High
general/tcp	Medium
80/tcp	Medium

. . . (continues) . . .

... (continued) ...

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

2.1.1 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)
used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result

```
Version of installed component:          22.7.2 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10
↪)
Latest available openvas-scanner version: 22.7.3
Reference URL(s) for the latest available version: https://forum.greenbone.net/t
↪/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
```

Solution:
Solution type: VendorFix
Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `Report outdated / end-of-life Scan Engine / Environment (local)`
OID:1.3.6.1.4.1.25623.1.0.108560
Version used: `2023-07-19T05:05:15Z`

References

```
url: https://www.greenbone.net/en/testnow/
url: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initi
↪al-release-2022-07-25/12638
url: https://forum.greenbone.net/t/greenbone-community-edition-21-04-end-of-life
↪/13837
url: https://forum.greenbone.net/t/gvm-21-04-end-of-life-initial-release-2021-04
↪-16/8942
url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08
↪-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14
↪/3674
url: https://forum.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-04-05
↪/208
url: https://forum.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03-07/
↪211
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#creating-an
↪-override
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.
- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108397
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:
- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108414
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.

. . . continues on next page . . .

... continued from previous page ...

- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108397
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108414

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-05-19T11:50:09Z

Product Detection Result
Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)

Product detection result
cpe:/a:oracle:jdk:1.6.0:update_41

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108399
Version used: `2022-08-09T10:11:17Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
url: http://www.securityfocus.com/bid/77200
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

... continues on next page ...

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to perform certain actions with escalated privileges, disclose sensitive information and compromise a user's system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors related to the Deployment subcomponent.
- An XXE (Xml eXternal Entity) injection error in com/sun/org/apache/xerces/internal/impl/XMLEntityManager.j script.
- An error in windows/native/sun/awt/splashscreen/splashscreen_sys.c script related to handling of splash images.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108414

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2014-6532
cve: CVE-2014-6517
cve: CVE-2014-6515
cve: CVE-2014-6513
cve: CVE-2014-6503
cve: CVE-2014-6493
cve: CVE-2014-6492
cve: CVE-2014-6466
cve: CVE-2014-6458
cve: CVE-2014-4288
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70456
url: http://www.securityfocus.com/bid/70460
url: http://www.securityfocus.com/bid/70468
url: http://www.securityfocus.com/bid/70470
url: http://www.securityfocus.com/bid/70484
url: http://www.securityfocus.com/bid/70507
url: http://www.securityfocus.com/bid/70518
url: http://www.securityfocus.com/bid/70552
url: http://www.securityfocus.com/bid/70565
url: http://www.securityfocus.com/bid/70569
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108399

Version used: `2022-08-09T10:11:17Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
url: http://www.securityfocus.com/bid/77200
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:

- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108401

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0412
cve: CVE-2015-0406
cve: CVE-2015-0403
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight
Multiple flaws exist:
- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108416
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 101 and prior, 7 update 85 and prior, 8 update 60 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2015 (Linux)
OID:1.3.6.1.4.1.25623.1.0.108399
Version used: 2022-08-09T10:11:17Z

Product Detection Result
Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

cve: CVE-2015-4902
cve: CVE-2015-4903
cve: CVE-2015-4911
cve: CVE-2015-4893
cve: CVE-2015-4883
cve: CVE-2015-4882
cve: CVE-2015-4881
cve: CVE-2015-4872
cve: CVE-2015-4860
cve: CVE-2015-4844
cve: CVE-2015-4843
cve: CVE-2015-4842
cve: CVE-2015-4835
cve: CVE-2015-4806
cve: CVE-2015-4805
cve: CVE-2015-4803
cve: CVE-2015-4734
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
url: http://www.securityfocus.com/bid/77241
url: http://www.securityfocus.com/bid/77194
url: http://www.securityfocus.com/bid/77209
url: http://www.securityfocus.com/bid/77207
url: http://www.securityfocus.com/bid/77161
url: http://www.securityfocus.com/bid/77181
url: http://www.securityfocus.com/bid/77159
url: http://www.securityfocus.com/bid/77211
url: http://www.securityfocus.com/bid/77162
url: http://www.securityfocus.com/bid/77164
url: http://www.securityfocus.com/bid/77160
url: http://www.securityfocus.com/bid/77154
url: http://www.securityfocus.com/bid/77148
url: http://www.securityfocus.com/bid/77126
url: http://www.securityfocus.com/bid/77163
url: http://www.securityfocus.com/bid/77200

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/77192
cert-bund: CB-K16/1842
cert-bund: CB-K16/1080
cert-bund: CB-K15/1759
cert-bund: CB-K15/1751
cert-bund: CB-K15/1713
cert-bund: CB-K15/1555
cert-bund: CB-K15/1552
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2015-1860
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1812
dfn-cert: DFN-CERT-2015-1641
dfn-cert: DFN-CERT-2015-1633
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:

. . . continues on next page . . .

. . . continued from previous page . . .

- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108401
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0412
cve: CVE-2015-0406
cve: CVE-2015-0403
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight

Multiple flaws exist:

- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108416

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain escalated privileges, conduct a denial of service attack, bypass sandbox restrictions and execute arbitrary code.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist due to:
- An unspecified error in the JAX-WS component related to insufficient privilege checks.
- Two unspecified errors in the Deployment component.
- An unspecified error in the 'Libraries' component.
- An error in vm/classfile/verifier.cpp script related to insufficient verification of invokespecial calls.
- A NULL pointer dereference error in the MulticastSocket implementation.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Feb 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108401
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
cve: CVE-2015-0412
cve: CVE-2015-0406
cve: CVE-2015-0403

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-0400
cve: CVE-2014-6601
cve: CVE-2014-6587
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72136
url: http://www.securityfocus.com/bid/72154
url: http://www.securityfocus.com/bid/72148
url: http://www.securityfocus.com/bid/72159
url: http://www.securityfocus.com/bid/72132
url: http://www.securityfocus.com/bid/72168
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0308
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to execute arbitrary code or possibly other impacts.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 75 and prior, 7 update 60 and prior, and 8 update 5.0 and prior on Linux.

Vulnerability Insight
Multiple flaws exist:
- Two unspecified errors related to the Deployment subcomponent.
- An unspecified error in the Hotspot subcomponent related to bytecode verification.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-03 Jul 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108416
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
```
cve: CVE-2014-4265
cve: CVE-2014-4219
cve: CVE-2014-4227
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68603
url: http://www.securityfocus.com/bid/68620
url: http://www.securityfocus.com/bid/68632
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:

- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108403

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:

- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108403

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to conduct a denial of service attack, man-in-the-middle attack, potentially disclose memory contents, remove or overwrite arbitrary files on the system, disclose certain directory information, bypass sandbox restrictions and potentially execute arbitrary code.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 75 and prior, 6 update 85 and prior, 7 update 72 and prior, and 8 update 25 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist due to:

- An infinite loop in the DER decoder that is triggered when handling negative length values.
- An error in the RMI component's transport implementation related to incorrect context class loader use.
- An error in the Swing component's file chooser implementation.
- An error in vm/memory/referenceProcessor.cpp related to handling of phantom object references in the Hotspot JVM garbage collector.
- An error in the Hotspot JVM related to insecure handling of temporary performance data files.
- An error in the JSSE component related to improper ChangeCipherSpec tracking during SSL/TLS handshakes.
- Two out-of-bounds read errors in the layout component that is triggered when parsing fonts.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 Feb 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108403

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-05-19T11:50:09Z

Product Detection Result
Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0410
cve: CVE-2015-0408
cve: CVE-2015-0407
cve: CVE-2015-0395
cve: CVE-2015-0383
cve: CVE-2014-6593
cve: CVE-2014-6591
cve: CVE-2014-6585
url: http://secunia.com/advisories/62215
url: http://www.securityfocus.com/bid/72165
url: http://www.securityfocus.com/bid/72140
url: http://www.securityfocus.com/bid/72162
url: http://www.securityfocus.com/bid/72142
url: http://www.securityfocus.com/bid/72155
url: http://www.securityfocus.com/bid/72169
url: http://www.securityfocus.com/bid/72175
url: http://www.securityfocus.com/bid/72173
url: http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
cert-bund: CB-K16/1739
cert-bund: CB-K15/1396
cert-bund: CB-K15/1133
cert-bund: CB-K15/0669
cert-bund: CB-K15/0442
cert-bund: CB-K15/0393
cert-bund: CB-K15/0316
cert-bund: CB-K15/0308
cert-bund: CB-K15/0291
cert-bund: CB-K15/0252
cert-bund: CB-K15/0237
cert-bund: CB-K15/0155
cert-bund: CB-K15/0108
cert-bund: CB-K15/0078
cert-bund: CB-K15/0077
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2015-1477
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-0701
dfn-cert: DFN-CERT-2015-0465
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0327
dfn-cert: DFN-CERT-2015-0318
dfn-cert: DFN-CERT-2015-0296
dfn-cert: DFN-CERT-2015-0259
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2015-0158
dfn-cert: DFN-CERT-2015-0114
dfn-cert: DFN-CERT-2015-0081
dfn-cert: DFN-CERT-2015-0076
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight

Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method

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

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)
OID:1.3.6.1.4.1.25623.1.0.108395
Version used: 2022-08-09T10:11:17Z

Product Detection Result
Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
cve: CVE-2015-2628
cve: CVE-2015-2632
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108412
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
cve: CVE-2013-5910
cve: CVE-2014-0375
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108415
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
cve: CVE-2014-0368
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/64932
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0596
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0146
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight
Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108395
Version used: `2022-08-09T10:11:17Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
cve: CVE-2015-2628
cve: CVE-2015-2632
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

Vulnerability Insight

Multiple unspecified vulnerabilities exist.

Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108412

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
cve: CVE-2013-5910
cve: CVE-2014-0375
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result
`The target host was found to be vulnerable`

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108415
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
cve: CVE-2014-0368
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
url: http://www.securityfocus.com/bid/64932
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0596
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0146
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior on Linux

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-02 Jan 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108412
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2013-5878
cve: CVE-2013-5887
cve: CVE-2013-5888
cve: CVE-2013-5889
cve: CVE-2013-5898
cve: CVE-2013-5899
cve: CVE-2013-5902
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2013-5910
cve: CVE-2014-0375
cve: CVE-2014-0410
cve: CVE-2014-0403
cve: CVE-2014-0415
cve: CVE-2014-0418
cve: CVE-2014-0424
cve: CVE-2014-0387
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64875
url: http://www.securityfocus.com/bid/64882
url: http://www.securityfocus.com/bid/64899
url: http://www.securityfocus.com/bid/64912
url: http://www.securityfocus.com/bid/64915
url: http://www.securityfocus.com/bid/64916
url: http://www.securityfocus.com/bid/64917
url: http://www.securityfocus.com/bid/64919
url: http://www.securityfocus.com/bid/64920
url: http://www.securityfocus.com/bid/64923
url: http://www.securityfocus.com/bid/64925
url: http://www.securityfocus.com/bid/64928
url: http://www.securityfocus.com/bid/64931
url: http://www.securityfocus.com/bid/64933
url: http://www.securityfocus.com/bid/64927
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 7 update 45 and prior, Java SE 6 update 65 and prior, Java SE 5 update 55 and prior on Linux.

Vulnerability Insight
Multiple unspecified vulnerabilities exist.
Please see the references for more information on the vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-03 Jan 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108415
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2013-5884
cve: CVE-2013-5896
cve: CVE-2013-5905
cve: CVE-2013-5906
cve: CVE-2013-5907
cve: CVE-2014-0368
cve: CVE-2014-0373
cve: CVE-2014-0376
cve: CVE-2014-0411
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2014-0416
cve: CVE-2014-0417
cve: CVE-2014-0422
cve: CVE-2014-0423
cve: CVE-2014-0428
url: http://secunia.com/advisories/56485
url: http://www.securityfocus.com/bid/64894
url: http://www.securityfocus.com/bid/64903
url: http://www.securityfocus.com/bid/64907
url: http://www.securityfocus.com/bid/64914
url: http://www.securityfocus.com/bid/64921
url: http://www.securityfocus.com/bid/64922
url: http://www.securityfocus.com/bid/64924
url: http://www.securityfocus.com/bid/64926
url: http://www.securityfocus.com/bid/64932
url: http://www.securityfocus.com/bid/64934
url: http://www.securityfocus.com/bid/64935
url: http://www.securityfocus.com/bid/64937
url: http://www.securityfocus.com/bid/64918
url: http://www.securityfocus.com/bid/64930
url: http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html
cert-bund: CB-K14/0728
cert-bund: CB-K14/0572
cert-bund: CB-K14/0477
cert-bund: CB-K14/0467
cert-bund: CB-K14/0176
cert-bund: CB-K14/0141
cert-bund: CB-K14/0140
cert-bund: CB-K14/0102
cert-bund: CB-K14/0053
cert-bund: CB-K14/0051
dfn-cert: DFN-CERT-2014-0755
dfn-cert: DFN-CERT-2014-0596
dfn-cert: DFN-CERT-2014-0475
dfn-cert: DFN-CERT-2014-0179
dfn-cert: DFN-CERT-2014-0146
dfn-cert: DFN-CERT-2014-0143
dfn-cert: DFN-CERT-2014-0050
dfn-cert: DFN-CERT-2014-0045
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

... continues on next page ...

. . . continued from previous page . . .

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact
Successful exploitation will allow attackers to gain knowledge of potentially sensitive information, conduct denial-of-service attacks, execute arbitrary code and other unspecified impact.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0 update 81 and prior, 6 update 91 and prior, 7 update 76 and prior, and 8 update 40 and prior on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- An error in the Java Cryptography Extension (JCE) subcomponent's RSA signature implementation.
- An error in the JSSE subcomponent that is triggered when checking X.509 certificate options.
- An error in the 'ReferenceProcessor::process_discovered_references' function in share/vm/memory/referenceProcessor.cpp script.
- Two unspecified errors related to the 2D subcomponent.
- An error in the Beans subcomponent related to permissions and resource loading.
- An off-by-one overflow condition in the functions 'LigatureSubstitutionProcessor::processStateEntry' and 'LigatureSubstitutionProcessor2::processStateEntry' within LigatureSubstProc.cpp and LigatureSubstProc2.cpp scripts respectively.
- An unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Apr 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108397
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

. . . continues on next page . . .

... continued from previous page ...

References

```
cve: CVE-2015-0491
cve: CVE-2015-0488
cve: CVE-2015-0480
cve: CVE-2015-0478
cve: CVE-2015-0477
cve: CVE-2015-0469
cve: CVE-2015-0460
cve: CVE-2015-0459
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74094
url: http://www.securityfocus.com/bid/74111
url: http://www.securityfocus.com/bid/74104
url: http://www.securityfocus.com/bid/74147
url: http://www.securityfocus.com/bid/74119
url: http://www.securityfocus.com/bid/74072
url: http://www.securityfocus.com/bid/74097
url: http://www.securityfocus.com/bid/74083
cert-bund: CB-K15/1751
cert-bund: CB-K15/1090
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0529
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0554
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch from the referenced advisory.
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 95, 7 update 80, 8 update 45 on Linux.

Vulnerability Insight

Multiple errors exist due to unspecified flaws related to multiple unspecified vectors.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 July 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108395

Version used: `2022-08-09T10:11:17Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-4760
cve: CVE-2015-4749
cve: CVE-2015-4748
cve: CVE-2015-4733
cve: CVE-2015-4732
cve: CVE-2015-4731
cve: CVE-2015-2664
cve: CVE-2015-2638
cve: CVE-2015-2637
cve: CVE-2015-2621
cve: CVE-2015-2625
cve: CVE-2015-2627
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-2628
cve: CVE-2015-2632
cve: CVE-2015-2601
cve: CVE-2015-2590
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
url: http://www.securityfocus.com/bid/75784
url: http://www.securityfocus.com/bid/75890
url: http://www.securityfocus.com/bid/75854
url: http://www.securityfocus.com/bid/75832
url: http://www.securityfocus.com/bid/75823
url: http://www.securityfocus.com/bid/75812
url: http://www.securityfocus.com/bid/75857
url: http://www.securityfocus.com/bid/75833
url: http://www.securityfocus.com/bid/75883
url: http://www.securityfocus.com/bid/75874
url: http://www.securityfocus.com/bid/75895
url: http://www.securityfocus.com/bid/75893
url: http://www.securityfocus.com/bid/75796
url: http://www.securityfocus.com/bid/75861
url: http://www.securityfocus.com/bid/75867
url: http://www.securityfocus.com/bid/75818
cert-bund: CB-K16/1842
cert-bund: CB-K16/0617
cert-bund: CB-K15/1751
cert-bund: CB-K15/1352
cert-bund: CB-K15/1302
cert-bund: CB-K15/1250
cert-bund: CB-K15/1249
cert-bund: CB-K15/1197
cert-bund: CB-K15/1148
cert-bund: CB-K15/1136
cert-bund: CB-K15/1133
cert-bund: CB-K15/1090
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1427
dfn-cert: DFN-CERT-2015-1373
dfn-cert: DFN-CERT-2015-1320
dfn-cert: DFN-CERT-2015-1318
dfn-cert: DFN-CERT-2015-1269
dfn-cert: DFN-CERT-2015-1206
dfn-cert: DFN-CERT-2015-1194
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1191
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108393
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
cert-bund: CB-K16/0065
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1274
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-1015
dfn-cert: DFN-CERT-2016-0554
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0484
dfn-cert: DFN-CERT-2016-0377
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-0358
dfn-cert: DFN-CERT-2016-0339
dfn-cert: DFN-CERT-2016-0288
dfn-cert: DFN-CERT-2016-0267
dfn-cert: DFN-CERT-2016-0100
dfn-cert: DFN-CERT-2016-0070
dfn-cert: DFN-CERT-2016-0001
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108393
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
cert-bund: CB-K16/0065
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2016-1947
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1274
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-1015
dfn-cert: DFN-CERT-2016-0554
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0484
dfn-cert: DFN-CERT-2016-0377
dfn-cert: DFN-CERT-2016-0358
dfn-cert: DFN-CERT-2016-0339
dfn-cert: DFN-CERT-2016-0288
dfn-cert: DFN-CERT-2016-0267
dfn-cert: DFN-CERT-2016-0100
dfn-cert: DFN-CERT-2016-0070
dfn-cert: DFN-CERT-2016-0001
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762
```

High (CVSS: 10.0)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity, and availability via unknown vectors.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 105, 7 update 91, 8 update 66 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to multiple unspecified errors.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jan 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108393
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0494
cve: CVE-2015-8126
cve: CVE-2016-0483
cve: CVE-2016-0402
cve: CVE-2016-0466
cve: CVE-2016-0448
cve: CVE-2015-7575
url: http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
cert-bund: WID-SEC-2023-0428
cert-bund: CB-K16/1842
cert-bund: CB-K16/1552
cert-bund: CB-K16/1201
cert-bund: CB-K16/1102
cert-bund: CB-K16/1080
cert-bund: CB-K16/0962
cert-bund: CB-K16/0509
cert-bund: CB-K16/0459
cert-bund: CB-K16/0446
cert-bund: CB-K16/0343
cert-bund: CB-K16/0327
cert-bund: CB-K16/0310
cert-bund: CB-K16/0262
cert-bund: CB-K16/0244
cert-bund: CB-K16/0089
cert-bund: CB-K16/0065
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/0001
cert-bund: CB-K15/1876
cert-bund: CB-K15/1839
cert-bund: CB-K15/1810
cert-bund: CB-K15/1803
cert-bund: CB-K15/1695
cert-bund: CB-K15/1666
dfn-cert: DFN-CERT-2016-1947
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1274
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-1015
dfn-cert: DFN-CERT-2016-0554
dfn-cert: DFN-CERT-2016-0496
dfn-cert: DFN-CERT-2016-0484
dfn-cert: DFN-CERT-2016-0377
dfn-cert: DFN-CERT-2016-0358
dfn-cert: DFN-CERT-2016-0339
dfn-cert: DFN-CERT-2016-0288
dfn-cert: DFN-CERT-2016-0267
dfn-cert: DFN-CERT-2016-0100
dfn-cert: DFN-CERT-2016-0070
dfn-cert: DFN-CERT-2016-0001
dfn-cert: DFN-CERT-2015-1984
dfn-cert: DFN-CERT-2015-1938
dfn-cert: DFN-CERT-2015-1907
dfn-cert: DFN-CERT-2015-1905
dfn-cert: DFN-CERT-2015-1789
dfn-cert: DFN-CERT-2015-1762
```

High (CVSS: 9.8)
NVT: Oracle Java SE Security Update (cpuoct2017 - 03) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight

Multiple flaws exist due to a flaw in Util (zlib) component of the application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuoct2017 - 03) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108380
Version used: `2022-06-24T09:38:38Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2022-0673
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2016-2109
```

High (CVSS: 9.8)
NVT: Oracle Java SE Security Update (cpuoct2017 - 03) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

. . . continues on next page . . .

... continued from previous page ...

Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight

Multiple flaws exist due to a flaw in Util (zlib) component of the application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Update (cpuoct2017 - 03) - Linux`
OID:1.3.6.1.4.1.25623.1.0.108380
Version used: `2022-06-24T09:38:38Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2022-0673
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-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: Oracle Java SE Security Update (cpuoct2017 - 03) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation of this vulnerability will allow attackers to partially modify data by leveraging improper pointer arithmetic within the application.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier.

Vulnerability Insight

Multiple flaws exist due to a flaw in Util (zlib) component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Update (cpuoct2017 - 03) - Linux`

OID:1.3.6.1.4.1.25623.1.0.108380

Version used: `2022-06-24T09:38:38Z`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-9841
url: https://www.oracle.com/security-alerts/cpuoct2017.html
url: http://www.securityfocus.com/bid/95131
cert-bund: WID-SEC-2022-0673
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-2019-0592
dfn-cert: DFN-CERT-2019-0463
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-0659
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1825
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1097
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2016-2109
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108375
Version used: `2023-03-24T10:19:42Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
cve: CVE-2017-10115
```

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
cve: CVE-2017-10243
cve: CVE-2017-10102
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- The Security component in ’OpenJDK’ failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in ’OpenJDK’ failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.

. . . continues on next page . . .

. . . continued from previous page . . .

- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108388
Version used: `2023-05-18T09:08:59Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
cert-bund: CB-K16/1080
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-0888
dfn-cert: DFN-CERT-2016-0860
dfn-cert: DFN-CERT-2016-0781
dfn-cert: DFN-CERT-2016-0683
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- The Security component in 'OpenJDK' failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in 'OpenJDK' failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.
- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108388

Version used: `2023-05-18T09:08:59Z`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
cert-bund: CB-K16/1080
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-0888
dfn-cert: DFN-CERT-2016-0860
dfn-cert: DFN-CERT-2016-0781
dfn-cert: DFN-CERT-2016-0683
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108375

Version used: `2023-03-24T10:19:42Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
cve: CVE-2017-10115
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2017-10243
cve: CVE-2017-10102
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108372

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

. . . continues on next page . . .

. . . continued from previous page . . .

Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/0939
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108372
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to have an impact on confidentiality, integrity and availability.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.151 and earlier, 1.7.0.141 and earlier, 1.8.0.131 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecifide errors in 'Security', 'AWT', 'ImageIO', 'JAXP', 'Libraries', 'RMI', 'Hotspot', 'JCE', 'JAX-WS', '2D', 'Serialization', 'Deployment' component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jul2017-3236622) 01 - Linux`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.108375
Version used: `2023-03-24T10:19:42Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10198
cve: CVE-2017-10096
cve: CVE-2017-10135
cve: CVE-2017-10110
cve: CVE-2017-10115
cve: CVE-2017-10116
cve: CVE-2017-10074
cve: CVE-2017-10053
cve: CVE-2017-10087
cve: CVE-2017-10089
cve: CVE-2017-10243
cve: CVE-2017-10102
cve: CVE-2017-10101
cve: CVE-2017-10107
cve: CVE-2017-10109
cve: CVE-2017-10105
cve: CVE-2017-10081
cve: CVE-2017-10193
cve: CVE-2017-10067
cve: CVE-2017-10108
url: http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
url: http://www.securityfocus.com/bid/99818
url: http://www.securityfocus.com/bid/99670
url: http://www.securityfocus.com/bid/99839
url: http://www.securityfocus.com/bid/99643
url: http://www.securityfocus.com/bid/99774
url: http://www.securityfocus.com/bid/99734
url: http://www.securityfocus.com/bid/99731
url: http://www.securityfocus.com/bid/99842
url: http://www.securityfocus.com/bid/99703
url: http://www.securityfocus.com/bid/99659
url: http://www.securityfocus.com/bid/99827
url: http://www.securityfocus.com/bid/99712
url: http://www.securityfocus.com/bid/99674
url: http://www.securityfocus.com/bid/99719
url: http://www.securityfocus.com/bid/99847
url: http://www.securityfocus.com/bid/99851
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/99853
url: http://www.securityfocus.com/bid/99854
url: http://www.securityfocus.com/bid/99756
url: http://www.securityfocus.com/bid/99846
cert-bund: CB-K18/0030
cert-bund: CB-K18/0015
cert-bund: CB-K17/2168
cert-bund: CB-K17/1699
cert-bund: CB-K17/1496
cert-bund: CB-K17/1477
cert-bund: CB-K17/1470
cert-bund: CB-K17/1375
cert-bund: CB-K17/1199
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2018-0014
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1775
dfn-cert: DFN-CERT-2017-1561
dfn-cert: DFN-CERT-2017-1543
dfn-cert: DFN-CERT-2017-1536
dfn-cert: DFN-CERT-2017-1438
dfn-cert: DFN-CERT-2017-1241
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight
Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108379
Version used: `2022-08-01T10:11:45Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10388
cve: CVE-2017-10293
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
cve: CVE-2017-10355
cve: CVE-2017-10357
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to:
- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries component.

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
cve: CVE-2016-5582
cve: CVE-2016-5573
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1908
dfn-cert: DFN-CERT-2016-1716
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation of this vulnerability will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.131 and earlier, 1.7.0.121 and earlier, 1.8.0.112 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'Libraries', 'RMI', '2D', 'JAAS', 'Networking' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2017-2881727) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108372
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-2183
cve: CVE-2017-3231
cve: CVE-2017-3261
cve: CVE-2016-5548
cve: CVE-2017-3253
cve: CVE-2017-3272
cve: CVE-2017-3252
cve: CVE-2017-3259
cve: CVE-2016-5552
cve: CVE-2016-5546
cve: CVE-2017-3241
url: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
url: http://www.securityfocus.com/bid/92630
url: http://www.securityfocus.com/bid/95563
url: http://www.securityfocus.com/bid/95566
url: http://www.securityfocus.com/bid/95559
url: http://www.securityfocus.com/bid/95498
url: http://www.securityfocus.com/bid/95533
url: http://www.securityfocus.com/bid/95509
url: http://www.securityfocus.com/bid/95570
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.securityfocus.com/bid/95512
url: http://www.securityfocus.com/bid/95506
url: http://www.securityfocus.com/bid/95488
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0892
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0211
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight

Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108379

Version used: `2022-08-01T10:11:45Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10388
cve: CVE-2017-10293
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
cve: CVE-2017-10355
cve: CVE-2017-10357
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Multiple flaws are due to:
- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
cve: CVE-2016-5582
cve: CVE-2016-5573
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1908
dfn-cert: DFN-CERT-2016-1716
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, also can obtain elevated privileges on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 121 and prior, 7 update 111 and prior, and 8 update 102 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to:

- A flaw in the 2D component.
- A flaw in the AWT component.
- A flaw in the Hotspot component.
- A flaw in the Networking component.
- A flaw in the JMX component.
- A flaw in the Libraries component.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 Oct 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108385
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-5556
cve: CVE-2016-5568
cve: CVE-2016-5582
cve: CVE-2016-5573
cve: CVE-2016-5597
cve: CVE-2016-5554
cve: CVE-2016-5542
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
url: http://www.securityfocus.com/bid/93618
url: http://www.securityfocus.com/bid/93621
url: http://www.securityfocus.com/bid/93623
url: http://www.securityfocus.com/bid/93628
cert-bund: CB-K17/0895
cert-bund: CB-K17/0892
cert-bund: CB-K17/0874
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0456
cert-bund: CB-K17/0055
cert-bund: CB-K16/1802
cert-bund: CB-K16/1615
dfn-cert: DFN-CERT-2017-0921
dfn-cert: DFN-CERT-2017-0920
dfn-cert: DFN-CERT-2017-0903
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0471
dfn-cert: DFN-CERT-2017-0060
dfn-cert: DFN-CERT-2016-1908
dfn-cert: DFN-CERT-2016-1716
```

High (CVSS: 9.6)
NVT: Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to gain elevated privileges, partially access and partially modify data, access sensitive data, obtain sensitive information or cause a denial of service, .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.161 and earlier, 1.7.0.151 and earlier, 1.8.0.144 and earlier, 9.0 on Linux.

Vulnerability Insight
Multiple flaws exist due to flaws in the 'Hotspot', 'RMI ', 'Libraries', 'Smart Card IO', 'Security', 'Javadoc', 'JAXP', 'Serialization' and 'Networking' components of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (oct2017-3236626) 02 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108379
Version used: `2022-08-01T10:11:45Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-10388
cve: CVE-2017-10293
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-10346
cve: CVE-2017-10345
cve: CVE-2017-10285
cve: CVE-2017-10356
cve: CVE-2017-10348
cve: CVE-2017-10295
cve: CVE-2017-10349
cve: CVE-2017-10347
cve: CVE-2017-10274
cve: CVE-2017-10355
cve: CVE-2017-10357
cve: CVE-2017-10281
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
url: http://www.securityfocus.com/bid/101321
url: http://www.securityfocus.com/bid/101338
url: http://www.securityfocus.com/bid/101315
url: http://www.securityfocus.com/bid/101396
url: http://www.securityfocus.com/bid/101319
url: http://www.securityfocus.com/bid/101413
url: http://www.securityfocus.com/bid/101354
url: http://www.securityfocus.com/bid/101384
url: http://www.securityfocus.com/bid/101348
url: http://www.securityfocus.com/bid/101382
url: http://www.securityfocus.com/bid/101333
url: http://www.securityfocus.com/bid/101369
url: http://www.securityfocus.com/bid/101355
url: http://www.securityfocus.com/bid/101378
cert-bund: CB-K18/0715
cert-bund: CB-K18/0570
cert-bund: CB-K18/0495
cert-bund: CB-K18/0301
cert-bund: CB-K18/0030
cert-bund: CB-K17/2199
cert-bund: CB-K17/2168
cert-bund: CB-K17/2106
cert-bund: CB-K17/2047
cert-bund: CB-K17/1745
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0691
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0643
dfn-cert: DFN-CERT-2018-0536
dfn-cert: DFN-CERT-2018-0318
dfn-cert: DFN-CERT-2018-0039
dfn-cert: DFN-CERT-2017-2300
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-2203
dfn-cert: DFN-CERT-2017-2135
dfn-cert: DFN-CERT-2017-1825
```

High (CVSS: 9.6)
NVT: Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via different vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 113 and prior, 7 update 99 and prior and 8 update 77 and prior on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- The Security component in 'OpenJDK' failed to check the digest algorithm strength when generating DSA signatures.
- The JAXP component in 'OpenJDK' failed to properly handle Unicode surrogate pairs used as part of the XML attribute values.
- The RMI server implementation in the JMX component in 'OpenJDK' did not restrict which classes can be deserialized when deserializing authentication credentials.
- Multiple unspecified vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

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

Details: `Oracle Java SE Multiple Vulnerabilities April 2016 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108388

Version used: `2023-05-18T09:08:59Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0695
cve: CVE-2016-0687
cve: CVE-2016-0686
cve: CVE-2016-3443
cve: CVE-2016-3427
cve: CVE-2016-3425
cve: CVE-2016-3422
cve: CVE-2016-3449
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.ht
↪ml
cert-bund: WID-SEC-2023-1214
cert-bund: CB-K17/0796
cert-bund: CB-K17/0090
cert-bund: CB-K16/1080
cert-bund: CB-K16/0800
cert-bund: CB-K16/0726
cert-bund: CB-K16/0634
cert-bund: CB-K16/0594
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0095
dfn-cert: DFN-CERT-2016-1148
dfn-cert: DFN-CERT-2016-0888
dfn-cert: DFN-CERT-2016-0860
dfn-cert: DFN-CERT-2016-0781
dfn-cert: DFN-CERT-2016-0683
dfn-cert: DFN-CERT-2016-0640
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)

Product detection result

`cpe:/a:oracle:jdk:1.6.0:update_41`

. . . continues on next page . . .

... continued from previous page ...

```
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result
```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist:
- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp
- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java
- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108410
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

... continues on next page ...

. . . continued from previous page . . .

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight
Multiple unspecified flaws exist:
- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp
- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108410
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 9.3)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to update, insert, or delete certain data, execute arbitrary code, conduct a denial of service and disclosure of potentially sensitive information.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 65 and prior, 6 update 75 and prior, 7 update 60 and prior, and 8 update 5 and prior on Linux.

Vulnerability Insight

Multiple unspecified flaws exist:

- An error in the JMX subcomponent related to share/classes/com/sun/jmx/remote/security/SubjectDelegator.java
- An error related to the Hotspot subcomponent in share/vm/classfile/classFileParser.hpp

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in the Libraries subcomponent related to share/classes/java/lang/reflect/Proxy.java and handling of interfaces passed to proxy methods.
- An error within the Swing subcomponent related to missing access restrictions imposed by the file choosers.
- An error in the Security subcomponent related to share/classes/java/security/Provider.java and instantiation of security services with non-public constructors.
- An error in the Diffie-Hellman key agreement within the Security subcomponent related to 'validateDHPublicKey' function in share/classes/sun/security/util/KeyUtil.java
- An error in Libraries subcomponent within 'AtomicReferenceFieldUpdaterImpl' function in /java/util/concurrent/atomic/AtomicReferenceFieldUpdater.java
- An error in the Security subcomponent related to share/classes/sun/security/rsa/RSACore.java and RSA 'blinding'.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Jul 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108410
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-4244
cve: CVE-2014-4262
cve: CVE-2014-4263
cve: CVE-2014-4252
cve: CVE-2014-4268
cve: CVE-2014-4218
cve: CVE-2014-4216
cve: CVE-2014-4209
url: http://secunia.com/advisories/59501
url: http://www.securityfocus.com/bid/68562
url: http://www.securityfocus.com/bid/68583
url: http://www.securityfocus.com/bid/68599
url: http://www.securityfocus.com/bid/68615
url: http://www.securityfocus.com/bid/68624
url: http://www.securityfocus.com/bid/68636
url: http://www.securityfocus.com/bid/68639
url: http://www.securityfocus.com/bid/68642
url: http://securitytracker.com/id?1030577
url: http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K14/1569
cert-bund: CB-K14/1507
cert-bund: CB-K14/1039
cert-bund: CB-K14/1038
cert-bund: CB-K14/0997
cert-bund: CB-K14/0984
cert-bund: CB-K14/0974
cert-bund: CB-K14/0930
cert-bund: CB-K14/0902
cert-bund: CB-K14/0878
cert-bund: CB-K14/0871
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1667
dfn-cert: DFN-CERT-2014-1595
dfn-cert: DFN-CERT-2014-1086
dfn-cert: DFN-CERT-2014-1085
dfn-cert: DFN-CERT-2014-1042
dfn-cert: DFN-CERT-2014-1029
dfn-cert: DFN-CERT-2014-1009
dfn-cert: DFN-CERT-2014-0972
dfn-cert: DFN-CERT-2014-0944
dfn-cert: DFN-CERT-2014-0918
dfn-cert: DFN-CERT-2014-0906
```

High (CVSS: 9.0)
NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight
The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813681
Version used: `2022-08-17T10:11:15Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 9.0)
NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight

The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`

OID:1.3.6.1.4.1.25623.1.0.813681

Version used: `2022-08-17T10:11:15Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 9.0)

NVT: Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

Oracle Java SE is prone to a remote privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to gain elevated privileges.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier on Linux

Vulnerability Insight

The flaw exists due to an unspecified error in 'Java DB' component.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-01 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813681
Version used: `2022-08-17T10:11:15Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2938
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1405
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE components

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813310

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE components

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813310
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 8.3)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

. . . continues on next page . . .

... continued from previous page ...

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.6.0.181 and earlier, 1.7.0.171 and earlier, 10.0 on Linux.

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in 'Hotspot', 'Security', 'AWT', 'JMX' and 'Serialization' Java SE components

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 04 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813310

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2814
cve: CVE-2018-2798
cve: CVE-2018-2797
cve: CVE-2018-2795
cve: CVE-2018-2790
cve: CVE-2018-2794
cve: CVE-2018-2815
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

High (CVSS: 7.8)
NVT: Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check

Product detection result

```
cpe:/a:sudo_project:sudo:1.8.9:p5
Detected by sudo / sudoers Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.25
↪623.1.0.117185)
```

Summary

Sudo is prone to a heap-based buffer overflow dubbed 'Baron Samedit'.

Vulnerability Detection Result

```
Used command: sudoedit -s '\' `perl -e 'print "A" x 65536'`
Result: sudoedit -s '' `perl -e 'print "A" x 65536'`
Segmentation fault
]0;vagrant@metasploitable3-ub1404: ~vagrant@metasploitable3-ub1404:~$
```

Solution:

Solution type: VendorFix

Update to version 1.9.5p2 or later.

Affected Software/OS

All legacy versions from 1.8.2 to 1.8.31p2 and all stable versions from 1.9.0 to 1.9.5p1 in their default configuration.

Vulnerability Insight

Sudo is allowing privilege escalation to root via 'sudoedit -s' and a command-line argument that ends with a single backslash character.

Vulnerability Detection Method

Runs a specific SSH command after the login to the target which is known to trigger an error message on affected versions of Sudo.

Details: `Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check`

OID:1.3.6.1.4.1.25623.1.0.117187

Version used: `2022-08-09T10:11:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:sudo_project:sudo:1.8.9:p5`
Method: `sudo / sudoers Detection (Linux/Unix SSH Login)`
OID: 1.3.6.1.4.1.25623.1.0.117185)

References

```
cve: CVE-2021-3156
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://www.sudo.ws/stable.html#1.9.5p2
url: https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-h
↪eap-based-buffer-overflow-in-sudo-baron-samedit
cert-bund: WID-SEC-2023-0066
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-0623
cert-bund: CB-K22/0130
cert-bund: CB-K21/0161
cert-bund: CB-K21/0092
dfn-cert: DFN-CERT-2022-0224
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0781
dfn-cert: DFN-CERT-2021-0299
dfn-cert: DFN-CERT-2021-0249
dfn-cert: DFN-CERT-2021-0202
dfn-cert: DFN-CERT-2021-0181
dfn-cert: DFN-CERT-2021-0180
dfn-cert: DFN-CERT-2021-0178
```

High (CVSS: 7.6)
NVT: Oracle Java SE Privilege Escalation Vulnerability (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

Vulnerability Insight
The flaw exists due to some unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Privilege Escalation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108389
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
dfn-cert: DFN-CERT-2016-0223
```

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight

The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108404

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0458
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
```

. . . continues on next page . . .

. . . continued from previous page . . .

`dfn-cert: DFN-CERT-2015-0544`

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight

The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108404
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

`cve: CVE-2015-0458`

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 7.6)
NVT: Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to an arbitrary code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
```

Impact

Successful exploitation will allow attackers to execute arbitrary code on affected system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 91 and prior, 7 update 76 and prior, 8 update 40 and prior on Linux.

Vulnerability Insight

The flaw is due to error related to the Deployment subcomponent.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Code Execution Vulnerability Apr 2015 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108404
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2015-0458
url: http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
url: http://www.securityfocus.com/bid/74141
cert-bund: CB-K15/1751
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0667
cert-bund: CB-K15/0550
cert-bund: CB-K15/0526
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2015-0572
dfn-cert: DFN-CERT-2015-0544
```

High (CVSS: 7.6)
NVT: Oracle Java SE Privilege Escalation Vulnerability (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

Vulnerability Insight
The flaw exists due to some unspecified error.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Privilege Escalation Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108389
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
dfn-cert: DFN-CERT-2016-0223
```

High (CVSS: 7.6)
NVT: Oracle Java SE Privilege Escalation Vulnerability (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to a privilege escalation vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to have an impact on confidentiality, integrity and availability via unknown vectors.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 111 and prior, 7 update 95 and prior, 8 update 71 and prior, and 8 update 72 and prior on Linux.

Vulnerability Insight

The flaw exists due to some unspecified error.

Vulnerability Detection Method

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

Details: `Oracle Java SE Privilege Escalation Vulnerability (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108389

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-0603
url: http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0603-28743
↪60.html
cert-bund: CB-K16/0197
dfn-cert: DFN-CERT-2016-0223
```

High (CVSS: 7.4)

NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in the 'Security' component of Java SE.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813307

Version used: `2022-10-10T10:12:14Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in the 'Security' component of Java SE.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813307
Version used: `2022-10-10T10:12:14Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
dfn-cert: DFN-CERT-2018-0102
```

High (CVSS: 7.4)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to a remote security vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

... continued from previous page ...

`path / port:` `/usr/lib/jvm/java-6-openjdk-amd64/bin/java`

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0.181 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in the 'Security' component of Java SE.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813307

Version used: `2022-10-10T10:12:14Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2783
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: WID-SEC-2023-0531
cert-bund: CB-K18/0882
cert-bund: CB-K18/0821
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1931
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1470
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-0724
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0102
```

[return to 10.0.0.10]

2.1.2 High 80/tcp

High (CVSS: 10.0)
NVT: Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check

Summary
Drupal is prone to a remote code execution (RCE) vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://ip-10-0-0-10.us-east-2.compute.internal/drupal/sites/all/
↪modules/coder/coder_upgrade/scripts/coder_upgrade.run.php
```

Solution:
Solution type: VendorFix
Install the latest version.

Vulnerability Insight
The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

Vulnerability Detection Method
Checks for known error message from affected modules.
Details: `Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105818
Version used: `2021-12-01T11:10:56Z`

References

```
url: https://www.drupal.org/node/2765575
```

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://ip-10-0-0-10.us-east-2.compute.internal/uploads/puttest333815460.html
We could delete the following files via the DELETE method at this web server:
http://ip-10-0-0-10.us-east-2.compute.internal/uploads/puttest333815460.html
```

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution:
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Affected Software/OS
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method
Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Details: `Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `2022-05-12T09:32:01Z`

References
```
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001
```

High (CVSS: 7.5)
NVT: Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

Summary
Drupal is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
```
Vulnerable URL: http://ip-10-0-0-10.us-east-2.compute.internal/drupal/?q=node&de
↪stination=node
```

Impact
Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Updates are available. Please see the references for more information.

Affected Software/OS
Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight
Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method
Sends a special crafted HTTP POST request and checks the response.
Details: `Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105101
Version used: `2022-04-14T11:24:11Z`

References

```
cve: CVE-2014-3704
url: https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-cor
↪e/2014-10-15/sa-core-2014-005-drupal-core-sql
url: http://www.securityfocus.com/bid/70595
cert-bund: CB-K14/1301
cert-bund: CB-K14/0920
dfn-cert: DFN-CERT-2014-1369
dfn-cert: DFN-CERT-2014-0958
```

[return to 10.0.0.10]

2.1.3 High package

High (CVSS: 10.0)
NVT: Ubuntu: Security Advisory (USN-4510-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4510-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm9
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'samba' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4510-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Tom Tervoort discovered that the Netlogon protocol implemented by Samba incorrectly handled the authentication scheme. A remote attacker could use this issue to forge an authentication token and steal the credentials of the domain admin.
This update fixes the issue by changing the 'server schannel' setting to default to 'yes', instead of 'auto', which will force a secure netlogon channel. This may result in compatibility issues with older devices. A future update may allow a finer-grained control over this setting.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4510-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4510.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4510-2
cve: CVE-2020-1472
advisory_id: USN-4510-2
cert-bund: CB-K21/0411
cert-bund: CB-K20/0816
dfn-cert: DFN-CERT-2021-2072
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-0827
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2020-2749
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2024
dfn-cert: DFN-CERT-2020-1768
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4014-2)

Summary
The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-4014-2 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.40.2-0ubuntu1.1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libglib2.0-0-2.40.2-0ubuntu1.1+esm1
```

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

Affected Software/OS
'glib2.0' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4014-1 fixed a vulnerability in GLib. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that GLib incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4014-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4014.2
Version used: `2023-03-27T04:11:00Z`

References

```
url: https://ubuntu.com/security/notices/USN-4014-2
cve: CVE-2019-12450
advisory_id: USN-4014-2
cert-bund: WID-SEC-2023-1156
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K19/0463
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2125
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1572
dfn-cert: DFN-CERT-2019-1274
dfn-cert: DFN-CERT-2019-1161
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4243-1)

Summary
The remote host is missing an update for the 'libbsd' package(s) announced via the USN-4243-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libbsd0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    libbsd0-0.6.0-2ubuntu1
Fixed version:      >=libbsd0-0.6.0-2ubuntu1+esm1
```

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

Affected Software/OS
'libbsd' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04.

Vulnerability Insight
It was discovered that libbsd incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 ESM. (CVE-2016-2090)
It was discovered that libbsd incorrectly handled certain strings. An attacker could possibly use this issue to access sensitive information. (CVE-2019-20367)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4243-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4243.1
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4243-1
cve: CVE-2016-2090
cve: CVE-2019-20367
advisory_id: USN-4243-1
cert-bund: CB-K16/2021
dfn-cert: DFN-CERT-2022-2672
dfn-cert: DFN-CERT-2020-0162
dfn-cert: DFN-CERT-2016-2132
```

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.

Vulnerability Detection Result
```
Vulnerable package:   libasn1-8-heimdal
Installed version:    libasn1-8-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libasn1-8-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm3
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm3
Vulnerable package:   libhx509-5-heimdal
Installed version:    libhx509-5-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libhx509-5-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm3
Vulnerable package:   libkrb5-26-heimdal
Installed version:    libkrb5-26-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libkrb5-26-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm3
```

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: `2023-01-13T04:10:42Z`

References

```
url: https://ubuntu.com/security/notices/USN-5800-1
cve: CVE-2021-44758
cve: CVE-2022-3437
cve: CVE-2022-42898
cve: CVE-2022-44640
advisory_id: USN-5800-1
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-2057
cert-bund: WID-SEC-2022-1847
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-5787-2)

Summary
The remote host is missing an update for the 'libksba' package(s) announced via the USN-5787-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libksba8
Installed version:    libksba8-1.3.0-3ubuntu0.14.04.2
Fixed version:      >=libksba8-1.3.0-3ubuntu0.14.04.2+esm2
```

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

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

Vulnerability Insight
USN-5787-1 fixed vulnerabilities in Libksba. This update provides the corresponding updates for Ubuntu 16.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
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-5787-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5787.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-01-09T13:35:04Z

References

```
url: https://ubuntu.com/security/notices/USN-5787-2
cve: CVE-2022-47629
advisory_id: USN-5787-2
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
dfn-cert: DFN-CERT-2022-2288
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5448-1)

Summary

The remote host is missing an update for the 'ncurses' package(s) announced via the USN-5448-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libncurses5
Installed version:    libncurses5-5.9+20140118-1ubuntu1
Fixed version:      >=libncurses5-5.9+20140118-1ubuntu1+esm1
Vulnerable package:   libncursesw5
Installed version:    libncursesw5-5.9+20140118-1ubuntu1
Fixed version:      >=libncursesw5-5.9+20140118-1ubuntu1+esm1
Vulnerable package:   libtinfo5
Installed version:    libtinfo5-5.9+20140118-1ubuntu1
Fixed version:      >=libtinfo5-5.9+20140118-1ubuntu1+esm1
Vulnerable package:   ncurses-base
Installed version:    ncurses-base-5.9+20140118-1ubuntu1
Fixed version:      >=ncurses-base-5.9+20140118-1ubuntu1+esm1
Vulnerable package:   ncurses-bin
Installed version:    ncurses-bin-5.9+20140118-1ubuntu1
Fixed version:      >=ncurses-bin-5.9+20140118-1ubuntu1+esm1
Vulnerable package:   ncurses-term
Installed version:    ncurses-term-5.9+20140118-1ubuntu1
Fixed version:      >=ncurses-term-5.9+20140118-1ubuntu1+esm1
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'ncurses' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that ncurses was not properly checking array bounds when executing the fmt_entry function, which could result in an out-of-bounds write. An attacker could possibly use this issue to execute arbitrary code. (CVE-2017-10684)
It was discovered that ncurses was not properly checking user input, which could result in it being treated as a format argument. An attacker could possibly use this issue to expose sensitive information or to execute arbitrary code. (CVE-2017-10685)
It was discovered that ncurses was incorrectly performing memory management operations and was not blocking access attempts to illegal memory locations. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-11112, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734)
It was discovered that ncurses was not properly performing checks on pointer values before attempting to access the related memory locations, which could lead to NULL pointer dereferencing. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-11113)
It was discovered that ncurses was incorrectly handling loops in libtic, which could lead to the execution of an infinite loop. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-13728)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5448-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5448.1
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-5448-1
cve: CVE-2017-10684
cve: CVE-2017-10685
cve: CVE-2017-11112
cve: CVE-2017-11113
cve: CVE-2017-13728
cve: CVE-2017-13729
cve: CVE-2017-13730
cve: CVE-2017-13731
cve: CVE-2017-13732
cve: CVE-2017-13733
cve: CVE-2017-13734
advisory_id: USN-5448-1
cert-bund: CB-K18/0143
cert-bund: CB-K18/0100
cert-bund: CB-K17/2095
cert-bund: CB-K17/1709
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1563
cert-bund: CB-K17/1139
dfn-cert: DFN-CERT-2022-1199
dfn-cert: DFN-CERT-2018-0156
dfn-cert: DFN-CERT-2018-0114
dfn-cert: DFN-CERT-2017-2190
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1630
dfn-cert: DFN-CERT-2017-1175
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4252-2)

Summary
The remote host is missing an update for the 'tcpdump' package(s) announced via the USN-4252-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   tcpdump
Installed version:    tcpdump-4.9.2-0ubuntu0.14.04.1
Fixed version:      >=tcpdump-4.9.3-0ubuntu0.14.04.1+esm1
```

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

Affected Software/OS
'tcpdump' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4252-1 fixed several vulnerabilities in tcpdump. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Multiple security issues were discovered in tcpdump. A remote attacker could use these issues to cause tcpdump 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-4252-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4252.2
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4252-2
cve: CVE-2017-16808
cve: CVE-2018-10103
```

. . . continues on next page . . .

. . . continued from previous page . . .

cve: CVE-2018-10105
cve: CVE-2018-14461
cve: CVE-2018-14462
cve: CVE-2018-14463
cve: CVE-2018-14464
cve: CVE-2018-14465
cve: CVE-2018-14466
cve: CVE-2018-14467
cve: CVE-2018-14468
cve: CVE-2018-14469
cve: CVE-2018-14470
cve: CVE-2018-14879
cve: CVE-2018-14880
cve: CVE-2018-14881
cve: CVE-2018-14882
cve: CVE-2018-16227
cve: CVE-2018-16228
cve: CVE-2018-16229
cve: CVE-2018-16230
cve: CVE-2018-16300
cve: CVE-2018-16451
cve: CVE-2018-16452
cve: CVE-2018-19519
cve: CVE-2019-1010220
cve: CVE-2019-15166
cve: CVE-2019-15167
advisory_id: USN-4252-2
cert-bund: WID-SEC-2022-2281
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0272
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K19/1065
cert-bund: CB-K19/0171
dfn-cert: DFN-CERT-2021-1191
dfn-cert: DFN-CERT-2020-2531
dfn-cert: DFN-CERT-2020-2394
dfn-cert: DFN-CERT-2020-0782
dfn-cert: DFN-CERT-2019-2621
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2143
dfn-cert: DFN-CERT-2019-2080
dfn-cert: DFN-CERT-2019-1951
dfn-cert: DFN-CERT-2019-1645
dfn-cert: DFN-CERT-2018-2561

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4754-5)

Summary

The remote host is missing an update for the 'python2.7' package(s) announced via the USN-4754-5 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm10
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm10
```

Solution:

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

Affected Software/OS

'python2.7' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-4754-1 fixed vulnerabilities in Python. Because of a regression, a subsequent update removed the fix for CVE-2021-3177. This update reinstates the security fix for CVE-2021-3177 in Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. (CVE-2020-27619, CVE-2021-3177)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4754-5)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.4754.5
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4754-5
cve: CVE-2020-27619
cve: CVE-2021-3177
advisory_id: USN-4754-5
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0495
cert-bund: CB-K22/0076
cert-bund: CB-K21/0782
dfn-cert: DFN-CERT-2023-1200
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-1438
dfn-cert: DFN-CERT-2022-0351
dfn-cert: DFN-CERT-2021-2350
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1541
dfn-cert: DFN-CERT-2021-1414
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1110
dfn-cert: DFN-CERT-2021-1080
dfn-cert: DFN-CERT-2021-1079
dfn-cert: DFN-CERT-2021-1071
dfn-cert: DFN-CERT-2021-1053
dfn-cert: DFN-CERT-2021-0810
dfn-cert: DFN-CERT-2021-0675
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0430
dfn-cert: DFN-CERT-2021-0367
dfn-cert: DFN-CERT-2021-0297
dfn-cert: DFN-CERT-2021-0151
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2757
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4754-2)

Summary
The remote host is missing an update for the 'python2.7' package(s) announced via the USN-4754-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm9
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm9
```

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

Affected Software/OS
'python2.7' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-4754-1 fixed a vulnerability in Python. The fix for CVE-2021-3177 introduced a regression in Python 2.7. This update reverts the security fix pending further investigation.
We apologize for the inconvenience.
Original advisory details:
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. (CVE-2020-27619, CVE-2021-3177)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4754-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4754.2
Version used: `2022-09-16T08:45:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4754-2
url: https://launchpad.net/bugs/1916893
cve: CVE-2020-27619
cve: CVE-2021-3177
advisory_id: USN-4754-2
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0495
cert-bund: CB-K22/0076
cert-bund: CB-K21/0782
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-1438
dfn-cert: DFN-CERT-2022-0351
dfn-cert: DFN-CERT-2021-2350
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1541
dfn-cert: DFN-CERT-2021-1414
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1110
dfn-cert: DFN-CERT-2021-1080
dfn-cert: DFN-CERT-2021-1079
dfn-cert: DFN-CERT-2021-1071
dfn-cert: DFN-CERT-2021-1053
dfn-cert: DFN-CERT-2021-0810
dfn-cert: DFN-CERT-2021-0675
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0430
dfn-cert: DFN-CERT-2021-0367
dfn-cert: DFN-CERT-2021-0297
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-0151
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2757
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4754-1)

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-4754-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm8
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm8
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm10
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm10
```

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, Ubuntu 20.10.

Vulnerability Insight
It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. (CVE-2020-27619, CVE-2021-3177)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4754-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4754.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-4754-1`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-27619
cve: CVE-2021-3177
advisory_id: USN-4754-1
cert-bund: WID-SEC-2022-0767
cert-bund: WID-SEC-2022-0495
cert-bund: CB-K22/0076
cert-bund: CB-K21/0782
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-1438
dfn-cert: DFN-CERT-2022-0351
dfn-cert: DFN-CERT-2021-2350
dfn-cert: DFN-CERT-2021-1801
dfn-cert: DFN-CERT-2021-1541
dfn-cert: DFN-CERT-2021-1414
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1110
dfn-cert: DFN-CERT-2021-1080
dfn-cert: DFN-CERT-2021-1079
dfn-cert: DFN-CERT-2021-1071
dfn-cert: DFN-CERT-2021-1053
dfn-cert: DFN-CERT-2021-0810
dfn-cert: DFN-CERT-2021-0675
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0430
dfn-cert: DFN-CERT-2021-0367
dfn-cert: DFN-CERT-2021-0297
dfn-cert: DFN-CERT-2021-0151
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2757
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4127-2)

Summary

The remote host is missing an update for the 'python2.7, python3.4' package(s) announced via the USN-4127-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm2
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm2
Vulnerable package:   python3.4
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:       >=python3.4-3.4.3-1ubuntu1~14.04.7+esm2
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:       >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm2
```

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

Affected Software/OS
'python2.7, python3.4' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4127-1 fixed several vulnerabilities in Python. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Python incorrectly handled certain pickle files. An attacker could possibly use this issue to consume memory, leading to a denial of service. This issue only affected Ubuntu 14.04 ESM. (CVE-2018-20406)
It was discovered that Python incorrectly validated the domain when handling cookies. An attacker could possibly trick Python into sending cookies to the wrong domain. (CVE-2018-20852)
Jonathan Birch and Panayiotis Panayiotou discovered that Python incorrectly handled Unicode encoding during NFKC normalization. An attacker could possibly use this issue to obtain sensitive information. (CVE-2019-9636, CVE-2019-10160)
Colin Read and Nicolas Edet discovered that Python incorrectly handled parsing certain X509 certificates. An attacker could possibly use this issue to cause Python to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 ESM. (CVE-2019-5010)
It was discovered that Python incorrectly handled certain urls. A remote attacker could possibly use this issue to perform CRLF injection attacks. (CVE-2019-9740, CVE-2019-9947)
Sihoon Lee discovered that Python incorrectly handled the local_file: scheme. A remote attacker could possibly use this issue to bypass blocklist meschanisms. (CVE-2019-9948)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4127-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4127.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4127-2
cve: CVE-2018-20406
cve: CVE-2018-20852
cve: CVE-2019-10160
cve: CVE-2019-5010
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-9636
cve: CVE-2019-9740
cve: CVE-2019-9947
cve: CVE-2019-9948
advisory_id: USN-4127-2
cert-bund: WID-SEC-2023-1280
cert-bund: CB-K20/1049
cert-bund: CB-K20/0109
cert-bund: CB-K20/0041
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2653
dfn-cert: DFN-CERT-2020-2621
dfn-cert: DFN-CERT-2020-2502
dfn-cert: DFN-CERT-2020-2259
dfn-cert: DFN-CERT-2020-2045
dfn-cert: DFN-CERT-2020-1839
dfn-cert: DFN-CERT-2020-1540
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0896
dfn-cert: DFN-CERT-2020-0783
dfn-cert: DFN-CERT-2020-0668
dfn-cert: DFN-CERT-2020-0231
dfn-cert: DFN-CERT-2020-0200
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2020-0102
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2327
dfn-cert: DFN-CERT-2019-2312
dfn-cert: DFN-CERT-2019-2302
dfn-cert: DFN-CERT-2019-2252
dfn-cert: DFN-CERT-2019-2238
dfn-cert: DFN-CERT-2019-2210
dfn-cert: DFN-CERT-2019-2198
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-2078
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1883
dfn-cert: DFN-CERT-2019-1877
dfn-cert: DFN-CERT-2019-1854
dfn-cert: DFN-CERT-2019-1831
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1682
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1610
dfn-cert: DFN-CERT-2019-1596
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1418
dfn-cert: DFN-CERT-2019-1370
dfn-cert: DFN-CERT-2019-1339
dfn-cert: DFN-CERT-2019-1288
dfn-cert: DFN-CERT-2019-1285
dfn-cert: DFN-CERT-2019-1263
dfn-cert: DFN-CERT-2019-1095
dfn-cert: DFN-CERT-2019-1084
dfn-cert: DFN-CERT-2019-1076
dfn-cert: DFN-CERT-2019-1053
dfn-cert: DFN-CERT-2019-0941
dfn-cert: DFN-CERT-2019-0915
dfn-cert: DFN-CERT-2019-0912
dfn-cert: DFN-CERT-2019-0841
dfn-cert: DFN-CERT-2019-0770
dfn-cert: DFN-CERT-2019-0702
dfn-cert: DFN-CERT-2019-0565
dfn-cert: DFN-CERT-2019-0402
dfn-cert: DFN-CERT-2019-0269
dfn-cert: DFN-CERT-2019-0221
dfn-cert: DFN-CERT-2019-0122
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-3188-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3188-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.108.116
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Andrey Konovalov discovered that the SCTP implementation in the Linux kernel improperly handled validation of incoming data. A remote attacker could use this to cause a denial of service (system crash).

. . . 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-3188-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3188.1
Version used: `2023-01-23T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-3188-1
cve: CVE-2016-9555
advisory_id: USN-3188-1
cert-bund: CB-K17/1901
cert-bund: CB-K17/0697
cert-bund: CB-K17/0332
cert-bund: CB-K17/0328
cert-bund: CB-K17/0297
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0201
cert-bund: CB-K17/0168
cert-bund: CB-K17/0094
cert-bund: CB-K16/1999
cert-bund: CB-K16/1936
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
cert-bund: CB-K16/1901
cert-bund: CB-K16/1900
cert-bund: CB-K16/1890
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2017-1986
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0338
dfn-cert: DFN-CERT-2017-0335
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0206
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0100
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2049
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2013
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-2004
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-3360-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3360-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.125.135
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that the Linux kernel did not properly initialize a Wake- on-Lan data structure. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2014-9900)
It was discovered that the Linux kernel did not properly restrict access to /proc/iomem. A local attacker could use this to expose sensitive information. (CVE-2015-8944)
It was discovered that a use-after-free vulnerability existed in the performance events and counters subsystem of the Linux kernel for ARM64. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2015-8955)
It was discovered that the SCSI generic (sg) driver in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2015-8962)
Sasha Levin discovered that a race condition existed in the performance events and counters subsystem of the Linux kernel when handling CPU unplug events. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2015-8963)
Tilman Schmidt and Sasha Levin discovered a use-after-free condition in the TTY implementation in the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2015-8964)
It was discovered that the fcntl64() system call in the Linux kernel did not properly set memory limits when returning on 32-bit ARM processors. A local attacker could use this to gain administrative privileges. (CVE-2015-8966)
It was discovered that the system call table for ARM 64-bit processors in the Linux kernel was not write-protected. An attacker could use this in conjunction with another kernel vulnerability to execute arbitrary code. (CVE-2015-8967)
It was discovered that the generic SCSI block layer in the Linux kernel did not properly restrict write operations in certain situations. A local attacker could use this to cause a denial of service (system crash) or possibly gain administrative privileges. (CVE-2016-10088)

... continues on next page ...

... continued from previous page ...

Alexander Potapenko discovered a race condition in the Advanced Linux Sound Architecture (ALSA) subsystem in the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2017-1000380)
Li Qiang discovered that the DRM driver for VMware Virtual GPUs in the Linux kernel did not properly validate some ioctl arguments. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-7346)
Tuomas Haanpaa and Ari Kauppi discovered that the NFSv2 and NFSv3 server implementations in the Linux kernel did not properly check for the end of buffer. A remote attacker could use this to craft requests that cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-7895)
It was discovered that an integer underflow existed in the Edgeport USB Serial ... [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-3360-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3360.1
Version used: `2023-01-23T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-3360-1
cve: CVE-2014-9900
cve: CVE-2015-8944
cve: CVE-2015-8955
cve: CVE-2015-8962
cve: CVE-2015-8963
cve: CVE-2015-8964
cve: CVE-2015-8966
cve: CVE-2015-8967
cve: CVE-2016-10088
cve: CVE-2017-1000380
cve: CVE-2017-7346
cve: CVE-2017-7895
cve: CVE-2017-8924
cve: CVE-2017-8925
cve: CVE-2017-9605
advisory_id: USN-3360-1
cert-bund: CB-K20/1030
cert-bund: CB-K18/0184
cert-bund: CB-K17/2192
cert-bund: CB-K17/2141
cert-bund: CB-K17/2124
cert-bund: CB-K17/2103
cert-bund: CB-K17/2080
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1849
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K17/1607
cert-bund: CB-K17/1584
cert-bund: CB-K17/1530
cert-bund: CB-K17/1520
cert-bund: CB-K17/1484
cert-bund: CB-K17/1408
cert-bund: CB-K17/1325
cert-bund: CB-K17/1286
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1243
cert-bund: CB-K17/1226
cert-bund: CB-K17/1225
cert-bund: CB-K17/1178
cert-bund: CB-K17/1102
cert-bund: CB-K17/1101
cert-bund: CB-K17/1085
cert-bund: CB-K17/1083
cert-bund: CB-K17/1034
cert-bund: CB-K17/1025
cert-bund: CB-K17/0941
cert-bund: CB-K17/0885
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0837
cert-bund: CB-K17/0834
cert-bund: CB-K17/0757
cert-bund: CB-K17/0697
cert-bund: CB-K17/0552
cert-bund: CB-K17/0484
cert-bund: CB-K17/0317
cert-bund: CB-K17/0297
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0260
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0168
cert-bund: CB-K17/0122
cert-bund: CB-K17/0088
cert-bund: CB-K16/1999
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
cert-bund: CB-K16/1900
cert-bund: CB-K16/1876
cert-bund: CB-K16/1740
cert-bund: CB-K16/1739
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1529
cert-bund: CB-K16/1526
cert-bund: CB-K16/1172
dfn-cert: DFN-CERT-2020-2632
dfn-cert: DFN-CERT-2020-2520
dfn-cert: DFN-CERT-2020-2219
dfn-cert: DFN-CERT-2020-2216
dfn-cert: DFN-CERT-2020-2186
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2020-0959
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2017-2291
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2196
dfn-cert: DFN-CERT-2017-2175
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1376
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1283
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-1268
dfn-cert: DFN-CERT-2017-1219
dfn-cert: DFN-CERT-2017-1140
dfn-cert: DFN-CERT-2017-1139
dfn-cert: DFN-CERT-2017-1120
dfn-cert: DFN-CERT-2017-1119
dfn-cert: DFN-CERT-2017-1070
dfn-cert: DFN-CERT-2017-1062
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0914
dfn-cert: DFN-CERT-2017-0867
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0776
dfn-cert: DFN-CERT-2017-0719
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0496
dfn-cert: DFN-CERT-2017-0322
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0265
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0124
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-1981
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2016-1843
dfn-cert: DFN-CERT-2016-1613
dfn-cert: DFN-CERT-2016-1612
dfn-cert: DFN-CERT-2016-1245
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-3754-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3754-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.157.167
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Ralf Spenneberg discovered that the ext4 implementation in the Linux kernel did not properly validate meta block groups. An attacker with physical access could use this to specially craft an ext4 image that causes a denial of service (system crash). (CVE-2016-10208)

. . . continues on next page . . .

... continued from previous page ...

It was discovered that an information disclosure vulnerability existed in the ACPI implementation of the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory addresses). (CVE-2017-11472)
It was discovered that a buffer overflow existed in the ACPI table parsing implementation in the Linux kernel. A local attacker could use this to construct a malicious ACPI table that, when loaded, caused a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-11473)
It was discovered that the generic SCSI driver in the Linux kernel did not properly initialize data returned to user space in some situations. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2017-14991)
It was discovered that a race condition existed in the packet fanout 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-2017-15649)
Andrey Konovalov discovered that the Ultra Wide Band driver in the Linux kernel did not properly check for an error condition. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-16526)
Andrey Konovalov discovered that the ALSA 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-2017-16527)
Andrey Konovalov discovered that the ALSA subsystem in the Linux kernel did not properly validate USB audio buffer descriptors. A physically proximate attacker could use this cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-16529)
Andrey Konovalov discovered that the USB subsystem in the Linux kernel did not properly validate USB interface association descriptors. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2017-16531)
Andrey Konovalov discovered that the usbtest device driver in the Linux kernel did not properly validate endpoint metadata. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2017-16532)
Andrey Konovalov discovered that the USB subsystem in the Linux kernel did not properly validate USB HID descriptors. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2017-16533)
Andrey Konovalov discovered that the USB subsystem in the Linux kernel did not properly validate USB BOS metadata. A physically proximate attacker could use this ... [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-3754-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3754.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3754-1
cve: CVE-2016-10208
cve: CVE-2017-11472
cve: CVE-2017-11473
cve: CVE-2017-14991
```

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2017-15649
cve: CVE-2017-16526
cve: CVE-2017-16527
cve: CVE-2017-16529
cve: CVE-2017-16531
cve: CVE-2017-16532
cve: CVE-2017-16533
cve: CVE-2017-16535
cve: CVE-2017-16536
cve: CVE-2017-16537
cve: CVE-2017-16538
cve: CVE-2017-16643
cve: CVE-2017-16644
cve: CVE-2017-16645
cve: CVE-2017-16650
cve: CVE-2017-16911
cve: CVE-2017-16912
cve: CVE-2017-16913
cve: CVE-2017-16914
cve: CVE-2017-17558
cve: CVE-2017-18255
cve: CVE-2017-18270
cve: CVE-2017-2583
cve: CVE-2017-2584
cve: CVE-2017-2671
cve: CVE-2017-5549
cve: CVE-2017-5897
cve: CVE-2017-6345
cve: CVE-2017-6348
cve: CVE-2017-7518
cve: CVE-2017-7645
cve: CVE-2017-8831
cve: CVE-2017-9984
cve: CVE-2017-9985
cve: CVE-2018-1000204
cve: CVE-2018-10021
cve: CVE-2018-10087
cve: CVE-2018-10124
cve: CVE-2018-10323
cve: CVE-2018-10675
cve: CVE-2018-10877
cve: CVE-2018-10881
cve: CVE-2018-1092
cve: CVE-2018-1093
cve: CVE-2018-10940
cve: CVE-2018-12233
cve: CVE-2018-13094
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-13405
cve: CVE-2018-13406
advisory_id: USN-3754-1
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-0959
cert-bund: WID-SEC-2022-0667
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K19/0774
cert-bund: CB-K19/0014
cert-bund: CB-K18/0936
cert-bund: CB-K18/0822
cert-bund: CB-K18/0763
cert-bund: CB-K18/0720
cert-bund: CB-K18/0701
cert-bund: CB-K18/0653
cert-bund: CB-K18/0651
cert-bund: CB-K18/0644
cert-bund: CB-K18/0635
cert-bund: CB-K18/0594
cert-bund: CB-K18/0553
cert-bund: CB-K18/0550
cert-bund: CB-K18/0523
cert-bund: CB-K18/0462
cert-bund: CB-K18/0405
cert-bund: CB-K18/0398
cert-bund: CB-K18/0364
cert-bund: CB-K18/0184
cert-bund: CB-K18/0173
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0080
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0040
cert-bund: CB-K18/0017
cert-bund: CB-K18/0014
cert-bund: CB-K18/0004
cert-bund: CB-K17/2223
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
cert-bund: CB-K17/2187
cert-bund: CB-K17/2182
cert-bund: CB-K17/2169
cert-bund: CB-K17/2146
cert-bund: CB-K17/2144
cert-bund: CB-K17/2141
cert-bund: CB-K17/2129
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/2125
cert-bund: CB-K17/2124
cert-bund: CB-K17/2098
cert-bund: CB-K17/2065
cert-bund: CB-K17/2055
cert-bund: CB-K17/2008
cert-bund: CB-K17/1998
cert-bund: CB-K17/1919
cert-bund: CB-K17/1908
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1850
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1837
cert-bund: CB-K17/1813
cert-bund: CB-K17/1812
cert-bund: CB-K17/1770
cert-bund: CB-K17/1696
cert-bund: CB-K17/1607
cert-bund: CB-K17/1584
cert-bund: CB-K17/1578
cert-bund: CB-K17/1567
cert-bund: CB-K17/1546
cert-bund: CB-K17/1530
cert-bund: CB-K17/1520
cert-bund: CB-K17/1505
cert-bund: CB-K17/1491
cert-bund: CB-K17/1484
cert-bund: CB-K17/1452
cert-bund: CB-K17/1381
cert-bund: CB-K17/1346
cert-bund: CB-K17/1323
cert-bund: CB-K17/1286
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1236
cert-bund: CB-K17/1226
cert-bund: CB-K17/1144
cert-bund: CB-K17/1105
cert-bund: CB-K17/1102
cert-bund: CB-K17/1101
cert-bund: CB-K17/1085
cert-bund: CB-K17/1083
cert-bund: CB-K17/1025
cert-bund: CB-K17/0961
cert-bund: CB-K17/0941
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0884
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0834
cert-bund: CB-K17/0826
cert-bund: CB-K17/0812
cert-bund: CB-K17/0773
cert-bund: CB-K17/0764
cert-bund: CB-K17/0746
cert-bund: CB-K17/0719
cert-bund: CB-K17/0691
cert-bund: CB-K17/0690
cert-bund: CB-K17/0648
cert-bund: CB-K17/0611
cert-bund: CB-K17/0552
cert-bund: CB-K17/0546
cert-bund: CB-K17/0458
cert-bund: CB-K17/0401
cert-bund: CB-K17/0354
cert-bund: CB-K17/0326
cert-bund: CB-K17/0325
cert-bund: CB-K17/0317
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0259
cert-bund: CB-K17/0247
cert-bund: CB-K17/0212
cert-bund: CB-K17/0157
cert-bund: CB-K17/0123
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2021-2560
dfn-cert: DFN-CERT-2021-2544
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-2517
dfn-cert: DFN-CERT-2021-2441
dfn-cert: DFN-CERT-2021-2425
dfn-cert: DFN-CERT-2021-2414
dfn-cert: DFN-CERT-2021-2315
dfn-cert: DFN-CERT-2021-0760
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2020-2186
dfn-cert: DFN-CERT-2020-1925
dfn-cert: DFN-CERT-2020-1894
dfn-cert: DFN-CERT-2020-1477
dfn-cert: DFN-CERT-2020-1041
dfn-cert: DFN-CERT-2020-0999
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0430
dfn-cert: DFN-CERT-2019-2614
dfn-cert: DFN-CERT-2019-2613
dfn-cert: DFN-CERT-2019-2459
dfn-cert: DFN-CERT-2019-2168
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-1907
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1702
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1008
dfn-cert: DFN-CERT-2019-1005
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0821
dfn-cert: DFN-CERT-2019-0727
dfn-cert: DFN-CERT-2019-0710
dfn-cert: DFN-CERT-2019-0708
dfn-cert: DFN-CERT-2019-0649
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0495
dfn-cert: DFN-CERT-2019-0245
dfn-cert: DFN-CERT-2019-0211
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0185
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0030
dfn-cert: DFN-CERT-2019-0027
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2019-0020
dfn-cert: DFN-CERT-2018-2512
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2497
dfn-cert: DFN-CERT-2018-2458
dfn-cert: DFN-CERT-2018-2442
dfn-cert: DFN-CERT-2018-2436
dfn-cert: DFN-CERT-2018-2335
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-2279
dfn-cert: DFN-CERT-2018-2233
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2118
dfn-cert: DFN-CERT-2018-2117
dfn-cert: DFN-CERT-2018-2067
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-2060
dfn-cert: DFN-CERT-2018-2050
dfn-cert: DFN-CERT-2018-2039
dfn-cert: DFN-CERT-2018-1997
dfn-cert: DFN-CERT-2018-1967
dfn-cert: DFN-CERT-2018-1966
dfn-cert: DFN-CERT-2018-1962
dfn-cert: DFN-CERT-2018-1943
dfn-cert: DFN-CERT-2018-1940
dfn-cert: DFN-CERT-2018-1905
dfn-cert: DFN-CERT-2018-1870
dfn-cert: DFN-CERT-2018-1863
dfn-cert: DFN-CERT-2018-1829
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1789
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1721
dfn-cert: DFN-CERT-2018-1720
dfn-cert: DFN-CERT-2018-1718
dfn-cert: DFN-CERT-2018-1677
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1654
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1632
dfn-cert: DFN-CERT-2018-1626
dfn-cert: DFN-CERT-2018-1623
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1544
dfn-cert: DFN-CERT-2018-1504
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1460
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1404
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1348
dfn-cert: DFN-CERT-2018-1337
dfn-cert: DFN-CERT-2018-1290
dfn-cert: DFN-CERT-2018-1288
dfn-cert: DFN-CERT-2018-1279
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1206
dfn-cert: DFN-CERT-2018-1205
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1190
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1179
dfn-cert: DFN-CERT-2018-1170
dfn-cert: DFN-CERT-2018-1124
dfn-cert: DFN-CERT-2018-1123
dfn-cert: DFN-CERT-2018-1122
dfn-cert: DFN-CERT-2018-1067
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-2018-0947
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0924
dfn-cert: DFN-CERT-2018-0915
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0910
dfn-cert: DFN-CERT-2018-0889
dfn-cert: DFN-CERT-2018-0884
dfn-cert: DFN-CERT-2018-0883
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0803
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0780
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0755
dfn-cert: DFN-CERT-2018-0713
dfn-cert: DFN-CERT-2018-0686
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0560
dfn-cert: DFN-CERT-2018-0500
dfn-cert: DFN-CERT-2018-0440
dfn-cert: DFN-CERT-2018-0427
dfn-cert: DFN-CERT-2018-0392
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0184
dfn-cert: DFN-CERT-2018-0181
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0095
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0016
dfn-cert: DFN-CERT-2018-0008
dfn-cert: DFN-CERT-2017-2319
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2286
dfn-cert: DFN-CERT-2017-2281
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2246
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2224
dfn-cert: DFN-CERT-2017-2223
dfn-cert: DFN-CERT-2017-2192
dfn-cert: DFN-CERT-2017-2162
dfn-cert: DFN-CERT-2017-2142
dfn-cert: DFN-CERT-2017-2099
dfn-cert: DFN-CERT-2017-2092
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1992
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1932
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1921
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1892
dfn-cert: DFN-CERT-2017-1851
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1646
dfn-cert: DFN-CERT-2017-1637
dfn-cert: DFN-CERT-2017-1617
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1570
dfn-cert: DFN-CERT-2017-1556
dfn-cert: DFN-CERT-2017-1551
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1518
dfn-cert: DFN-CERT-2017-1444
dfn-cert: DFN-CERT-2017-1405
dfn-cert: DFN-CERT-2017-1372
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1278
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-1183
dfn-cert: DFN-CERT-2017-1140
dfn-cert: DFN-CERT-2017-1139
dfn-cert: DFN-CERT-2017-1137
dfn-cert: DFN-CERT-2017-1120
dfn-cert: DFN-CERT-2017-1119
dfn-cert: DFN-CERT-2017-1062
dfn-cert: DFN-CERT-2017-0995
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0912
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0799
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0771
dfn-cert: DFN-CERT-2017-0743
dfn-cert: DFN-CERT-2017-0713
dfn-cert: DFN-CERT-2017-0712
dfn-cert: DFN-CERT-2017-0666
dfn-cert: DFN-CERT-2017-0622
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0474
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0359
dfn-cert: DFN-CERT-2017-0331
dfn-cert: DFN-CERT-2017-0327
dfn-cert: DFN-CERT-2017-0322
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0264
dfn-cert: DFN-CERT-2017-0247
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0158
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0126
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-3583-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3583-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.142.152
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that an out-of-bounds write vulnerability existed in the Flash-Friendly File System (f2fs) in the Linux kernel. An attacker could construct a malicious file system that, when mounted, could cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-0750)
It was discovered that a race condition leading to a use-after-free vulnerability existed in the ALSA PCM subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-0861)
It was discovered that the KVM implementation in the Linux kernel allowed passthrough of the diagnostic I/O port 0x80. An attacker in a guest VM could use this to cause a denial of service (system crash) in the host OS. (CVE-2017-1000407)
Bo Zhang discovered that the netlink wireless configuration interface in the Linux kernel did not properly validate attributes when handling certain requests. A local attacker with the CAP_NET_ADMIN could use this to cause a denial of service (system crash). (CVE-2017-12153)
Vitaly Mayatskikh discovered that the SCSI subsystem in the Linux kernel did not properly track reference counts when merging buffers. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2017-12190)
It was discovered that the key management subsystem in the Linux kernel did not properly restrict key reads on negatively instantiated keys. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-12192)
It was discovered that an integer overflow existed in the sysfs interface for the QLogic 24xx+ series SCSI driver in the Linux kernel. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2017-14051)

. . . continues on next page . . .

. . . continued from previous page . . .

Otto Ebeling discovered that the memory manager in the Linux kernel did not properly check the effective UID in some situations. A local attacker could use this to expose sensitive information. (CVE-2017-14140)
It was discovered that the ATI Radeon framebuffer driver in the Linux kernel did not properly initialize a data structure returned to user space. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2017-14156)
ChunYu Wang discovered that the iSCSI transport implementation in the Linux kernel did not properly validate data structures. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-14489)
James Patrick-Evans discovered a race condition in the LEGO USB Infrared Tower driver in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-15102)
ChunYu Wang discovered that a use-after-free vulnerability existed in the SCTP protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system ... [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-3583-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3583.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3583-1
cve: CVE-2017-0750
cve: CVE-2017-0861
cve: CVE-2017-1000407
cve: CVE-2017-12153
cve: CVE-2017-12190
cve: CVE-2017-12192
cve: CVE-2017-14051
cve: CVE-2017-14140
cve: CVE-2017-14156
cve: CVE-2017-14489
cve: CVE-2017-15102
cve: CVE-2017-15115
cve: CVE-2017-15274
cve: CVE-2017-15868
cve: CVE-2017-16525
cve: CVE-2017-17450
cve: CVE-2017-17806
cve: CVE-2017-18017
cve: CVE-2017-5669
cve: CVE-2017-5754
cve: CVE-2017-7542
cve: CVE-2017-7889
cve: CVE-2017-8824
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-5333
cve: CVE-2018-5344
advisory_id: USN-3583-1
cert-bund: WID-SEC-2023-0531
cert-bund: WID-SEC-2023-0527
cert-bund: WID-SEC-2023-0526
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0667
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K20/0324
cert-bund: CB-K18/1140
cert-bund: CB-K18/0898
cert-bund: CB-K18/0701
cert-bund: CB-K18/0654
cert-bund: CB-K18/0651
cert-bund: CB-K18/0635
cert-bund: CB-K18/0557
cert-bund: CB-K18/0550
cert-bund: CB-K18/0472
cert-bund: CB-K18/0463
cert-bund: CB-K18/0462
cert-bund: CB-K18/0404
cert-bund: CB-K18/0398
cert-bund: CB-K18/0381
cert-bund: CB-K18/0370
cert-bund: CB-K18/0367
cert-bund: CB-K18/0364
cert-bund: CB-K18/0348
cert-bund: CB-K18/0347
cert-bund: CB-K18/0346
cert-bund: CB-K18/0338
cert-bund: CB-K18/0283
cert-bund: CB-K18/0257
cert-bund: CB-K18/0250
cert-bund: CB-K18/0244
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0183
cert-bund: CB-K18/0177
cert-bund: CB-K18/0166
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0148
cert-bund: CB-K18/0132
cert-bund: CB-K18/0129
cert-bund: CB-K18/0080
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0054
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
cert-bund: CB-K18/0022
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0014
cert-bund: CB-K18/0010
cert-bund: CB-K18/0004
cert-bund: CB-K17/2223
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
cert-bund: CB-K17/2187
cert-bund: CB-K17/2169
cert-bund: CB-K17/2146
cert-bund: CB-K17/2144
cert-bund: CB-K17/2141
cert-bund: CB-K17/2125
cert-bund: CB-K17/2124
cert-bund: CB-K17/2117
cert-bund: CB-K17/2113
cert-bund: CB-K17/2103
cert-bund: CB-K17/2098
cert-bund: CB-K17/2081
cert-bund: CB-K17/2008
cert-bund: CB-K17/1998
cert-bund: CB-K17/1986
cert-bund: CB-K17/1940
cert-bund: CB-K17/1919
cert-bund: CB-K17/1908
cert-bund: CB-K17/1905
cert-bund: CB-K17/1892
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1867
cert-bund: CB-K17/1850
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1813
cert-bund: CB-K17/1804
cert-bund: CB-K17/1776
cert-bund: CB-K17/1772
cert-bund: CB-K17/1770
cert-bund: CB-K17/1769
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1742
cert-bund: CB-K17/1708
cert-bund: CB-K17/1696
cert-bund: CB-K17/1607
cert-bund: CB-K17/1584
cert-bund: CB-K17/1568
cert-bund: CB-K17/1567
cert-bund: CB-K17/1532
cert-bund: CB-K17/1530
cert-bund: CB-K17/1521
cert-bund: CB-K17/1520
cert-bund: CB-K17/1484
cert-bund: CB-K17/1452
cert-bund: CB-K17/1408
cert-bund: CB-K17/1376
cert-bund: CB-K17/1346
cert-bund: CB-K17/1329
cert-bund: CB-K17/1325
cert-bund: CB-K17/1286
cert-bund: CB-K17/1236
cert-bund: CB-K17/1226
cert-bund: CB-K17/0941
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0834
cert-bund: CB-K17/0826
cert-bund: CB-K17/0812
cert-bund: CB-K17/0691
cert-bund: CB-K17/0690
cert-bund: CB-K17/0546
cert-bund: CB-K17/0403
cert-bund: CB-K17/0401
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2022-1570
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0095
dfn-cert: DFN-CERT-2020-1242
dfn-cert: DFN-CERT-2020-0023
dfn-cert: DFN-CERT-2019-2459
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-1554
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0245
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0027
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2550
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2497
dfn-cert: DFN-CERT-2018-2465
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-2287
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-1794
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1569
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1404
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1337
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1179
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1067
dfn-cert: DFN-CERT-2018-1025
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0947
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0924
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0911
dfn-cert: DFN-CERT-2018-0889
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0808
dfn-cert: DFN-CERT-2018-0799
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0737
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0605
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0500
dfn-cert: DFN-CERT-2018-0499
dfn-cert: DFN-CERT-2018-0439
dfn-cert: DFN-CERT-2018-0427
dfn-cert: DFN-CERT-2018-0410
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0392
dfn-cert: DFN-CERT-2018-0377
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0367
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0267
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0198
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0182
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0163
dfn-cert: DFN-CERT-2018-0143
dfn-cert: DFN-CERT-2018-0137
dfn-cert: DFN-CERT-2018-0095
dfn-cert: DFN-CERT-2018-0066
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2018-0016
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0008
dfn-cert: DFN-CERT-2017-2319
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2286
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2246
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2224
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-2210
dfn-cert: DFN-CERT-2017-2196
dfn-cert: DFN-CERT-2017-2192
dfn-cert: DFN-CERT-2017-2176
dfn-cert: DFN-CERT-2017-2099
dfn-cert: DFN-CERT-2017-2092
dfn-cert: DFN-CERT-2017-2064
dfn-cert: DFN-CERT-2017-2023
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1992
dfn-cert: DFN-CERT-2017-1989
dfn-cert: DFN-CERT-2017-1972
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1932
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1887
dfn-cert: DFN-CERT-2017-1852
dfn-cert: DFN-CERT-2017-1851
dfn-cert: DFN-CERT-2017-1850
dfn-cert: DFN-CERT-2017-1847
dfn-cert: DFN-CERT-2017-1820
dfn-cert: DFN-CERT-2017-1787
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1637
dfn-cert: DFN-CERT-2017-1632
dfn-cert: DFN-CERT-2017-1598
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1588
dfn-cert: DFN-CERT-2017-1583
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1518
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1439
dfn-cert: DFN-CERT-2017-1405
dfn-cert: DFN-CERT-2017-1378
dfn-cert: DFN-CERT-2017-1376
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1278
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0713
dfn-cert: DFN-CERT-2017-0712
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0408
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-3620-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3620-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.144.154
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the netlink 802.11 configuration interface in the Linux kernel did not properly validate some attributes passed from userspace. A local attacker with the CAP_NET_ADMIN privilege could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-11089)
It was discovered that a buffer overflow existed in the ioctl handling code in the ISDN subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-12762)
It was discovered that the netfilter component of the Linux did not properly restrict access to the connection tracking helpers list. A local attacker could use this to bypass intended access restrictions. (CVE-2017-17448)
Dmitry Vyukov discovered that the KVM implementation in the Linux kernel contained an out-of-bounds read when handling memory-mapped I/O. A local attacker could use this to expose sensitive information. (CVE-2017-17741)
It was discovered that the Salsa20 encryption algorithm implementations in the Linux kernel did not properly handle zero-length inputs. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-17805)
It was discovered that the keyring implementation in the Linux kernel did not properly check permissions when a key request was performed on a task's default keyring. A local attacker could use this to add keys to unauthorized keyrings. (CVE-2017-17807)
It was discovered that the Broadcom NetXtremeII ethernet driver in the Linux kernel did not properly validate Generic Segment Offload (GSO) packet sizes. An attacker could use this to cause a denial of service (interface unavailability). (CVE-2018-1000026)
It was discovered that the Reliable Datagram Socket (RDS) implementation in the Linux kernel contained an out-of-bounds write during RDMA page allocation. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-5332)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3620-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3620.1
Version used: `2023-01-23T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-3620-1
cve: CVE-2017-11089
cve: CVE-2017-12762
cve: CVE-2017-17448
cve: CVE-2017-17741
cve: CVE-2017-17805
cve: CVE-2017-17807
cve: CVE-2018-1000026
cve: CVE-2018-5332
advisory_id: USN-3620-1
cert-bund: WID-SEC-2023-0527
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K18/0701
cert-bund: CB-K18/0635
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0550
cert-bund: CB-K18/0523
cert-bund: CB-K18/0367
cert-bund: CB-K18/0347
cert-bund: CB-K18/0329
cert-bund: CB-K18/0250
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0132
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0040
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K17/2223
cert-bund: CB-K17/2213
cert-bund: CB-K17/2212
cert-bund: CB-K17/2193
cert-bund: CB-K17/2187
cert-bund: CB-K17/2144
cert-bund: CB-K17/1905
cert-bund: CB-K17/1892
cert-bund: CB-K17/1849
cert-bund: CB-K17/1792
cert-bund: CB-K17/1781
cert-bund: CB-K17/1696
cert-bund: CB-K17/1584
cert-bund: CB-K17/1578
dfn-cert: DFN-CERT-2021-2279
dfn-cert: DFN-CERT-2020-0661
dfn-cert: DFN-CERT-2020-0659
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-1701
dfn-cert: DFN-CERT-2019-1025
dfn-cert: DFN-CERT-2019-0894
dfn-cert: DFN-CERT-2019-0497
dfn-cert: DFN-CERT-2019-0495
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2497
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-1941
dfn-cert: DFN-CERT-2018-1404
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1228
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1206
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1179
dfn-cert: DFN-CERT-2018-1170
dfn-cert: DFN-CERT-2018-1067
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0932
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0560
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0353
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0143
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2017-2319
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2313
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2286
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-1989
dfn-cert: DFN-CERT-2017-1972
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1867
dfn-cert: DFN-CERT-2017-1862
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1646
```

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.1.0-4ubuntu1.4
Fixed version:      >=libexpat1-2.1.0-4ubuntu1.4+esm4
```

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: `2022-09-13T14:14:11Z`

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-2023-0132
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2022-0798
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-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
dfn-cert: DFN-CERT-2022-0486
dfn-cert: DFN-CERT-2022-0450
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-5320-1)

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

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.1.0-4ubuntu1.4
Fixed version:      >=libexpat1-2.1.0-4ubuntu1.4+esm6
```

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: `2022-09-13T14:14:11Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-5320-1
url: https://launchpad.net/bugs/1963903
cve: CVE-2022-25236
cve: CVE-2022-25313
cve: CVE-2022-25314
cve: CVE-2022-25315
advisory_id: USN-5320-1
cert-bund: WID-SEC-2023-1021
cert-bund: WID-SEC-2023-0137
cert-bund: WID-SEC-2023-0132
cert-bund: WID-SEC-2022-1772
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
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: WID-SEC-2022-0062
cert-bund: CB-K22/0220
cert-bund: CB-K22/0208
dfn-cert: DFN-CERT-2023-0832
dfn-cert: DFN-CERT-2023-0119
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-2022-0732
dfn-cert: DFN-CERT-2022-0669
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2022-0623
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2022-0412
dfn-cert: DFN-CERT-2022-0404
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libksba8
Installed version:    libksba8-1.3.0-3ubuntu0.14.04.2
Fixed version:      >=libksba8-1.3.0-3ubuntu0.14.04.2+esm1
```

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: `2023-01-23T04:10:55Z`

References

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

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2022-2288

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4624-1)

Summary
The remote host is missing an update for the 'libexif' package(s) announced via the USN-4624-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexif12
Installed version:    libexif12-0.6.21-1ubuntu1
Fixed version:      >=libexif12-0.6.21-1ubuntu1+esm6
```

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

Affected Software/OS
'libexif' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10.

Vulnerability Insight
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause unexpected behaviours, or execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-4624-1)
OID:1.3.6.1.4.1.25623.1.1.12.2020.4624.1
Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4624-1
cve: CVE-2020-0452
advisory_id: USN-4624-1
cert-bund: CB-K20/1062
dfn-cert: DFN-CERT-2020-2600
dfn-cert: DFN-CERT-2020-2455
dfn-cert: DFN-CERT-2020-2442
dfn-cert: DFN-CERT-2020-2379
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4004-2)

Summary
The remote host is missing an update for the 'db5.3' package(s) announced via the USN-4004-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libdb5.3
Installed version:    libdb5.3-5.3.28-3ubuntu3.1
Fixed version:      >=libdb5.3-5.3.28-3ubuntu3.1+esm1
```

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

Affected Software/OS
'db5.3' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4004-1 fixed a vulnerability in Berkeley DB. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Berkeley DB incorrectly handled certain inputs. An attacker could possibly use this issue to read sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4004-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4004.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4004-2
cve: CVE-2019-8457
advisory_id: USN-4004-2
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-0582
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/0988
cert-bund: CB-K20/0287
cert-bund: CB-K20/0038
cert-bund: CB-K19/0915
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2005
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2252
dfn-cert: DFN-CERT-2020-1528
dfn-cert: DFN-CERT-2020-1325
dfn-cert: DFN-CERT-2020-0890
dfn-cert: DFN-CERT-2020-0710
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1248
dfn-cert: DFN-CERT-2019-1211
dfn-cert: DFN-CERT-2019-1125
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4218-1)

Summary
The remote host is missing an update for the 'eglibc' package(s) announced via the USN-4218-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libc6
Installed version:    libc6-2.19-0ubuntu6.15
Fixed version:      >=libc6-2.19-0ubuntu6.15+esm1
```

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

Affected Software/OS
'eglibc' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
Jakub Wilk discovered that GNU C Library incorrectly handled certain memory alignments. 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-4218-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4218.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4218-1
cve: CVE-2018-6485
advisory_id: USN-4218-1
cert-bund: CB-K18/0295
dfn-cert: DFN-CERT-2020-1455
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-2596
dfn-cert: DFN-CERT-2018-2209
dfn-cert: DFN-CERT-2018-0319
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4288-2)

Summary
The remote host is missing an update for the 'ppp' package(s) announced via the USN-4288-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ppp
Installed version:    ppp-2.4.5-5.1ubuntu2.3
Fixed version:      >=ppp-2.4.5-5.1ubuntu2.3+esm1
```

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

Affected Software/OS
'ppp' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4288-1 fixed a vulnerability in ppp. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that ppp incorrectly handled certain rhostname values. A remote attacker could use this issue to cause ppp 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-4288-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4288.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4288-2
cve: CVE-2020-8597
advisory_id: USN-4288-2
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/0517
cert-bund: CB-K20/0166
dfn-cert: DFN-CERT-2020-1710
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-1151
dfn-cert: DFN-CERT-2020-0729
dfn-cert: DFN-CERT-2020-0555
dfn-cert: DFN-CERT-2020-0282
```

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

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

Vulnerability Detection Result

```
Vulnerable package:   libpam-modules
Installed version:    libpam-modules-1.1.8-1ubuntu2.2
Fixed version:      >=libpam-modules-1.1.8-1ubuntu2.2+esm3
```

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

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

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

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

References

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

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4309-1)

Summary
The remote host is missing an update for the ’vim’ package(s) announced via the USN-4309-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   vim-common
Installed version:    vim-common-2:7.4.052-1ubuntu3.1
Fixed version:      >=vim-common-2:7.4.052-1ubuntu3.1+esm1
```

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

Affected Software/OS
’vim’ package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that Vim incorrectly handled certain sources. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS (CVE-2017-11109)
It was discovered that Vim incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. (CVE-2017-5953)
It was discovered that Vim incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.06 LTS. (CVE-2018-20786)
It was discovered that Vim incorrectly handled certain inputs. 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 19.10. (CVE-2019-20079)
It was discovered that Vim incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2017-6349, CVE-2017-6350)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4309-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4309.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4309-1
cve: CVE-2017-11109
cve: CVE-2017-5953
cve: CVE-2017-6349
cve: CVE-2017-6350
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-20786
cve: CVE-2019-20079
advisory_id: USN-4309-1
cert-bund: WID-SEC-2023-0029
cert-bund: WID-SEC-2022-2407
cert-bund: WID-SEC-2022-2406
cert-bund: CB-K17/1090
cert-bund: CB-K17/0362
dfn-cert: DFN-CERT-2022-2921
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-0596
dfn-cert: DFN-CERT-2019-1581
dfn-cert: DFN-CERT-2019-1177
dfn-cert: DFN-CERT-2017-1126
dfn-cert: DFN-CERT-2017-0372
dfn-cert: DFN-CERT-2017-0260
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4994-2)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-4994-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm1
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm1
```

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

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

Vulnerability Insight
USN-4994-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
Antonio Morales discovered that the Apache mod_auth_digest module incorrectly handled certain Digest nonces. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. (CVE-2020-35452)

. . . continues on next page . . .

. . . continued from previous page . . .

Antonio Morales discovered that the Apache mod_session module incorrectly handled certain Cookie headers. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. (CVE-2021-26690)

Christophe Jaillet discovered that the Apache mod_session module incorrectly handled certain SessionHeader values. A remote attacker could use this issue to cause Apache to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-26691)

Christoph Anton Mitterer discovered that the new MergeSlashes configuration option resulted in unexpected behaviour in certain situations. (CVE-2021-30641)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-4994-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.4994.2

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4994-2
cve: CVE-2020-35452
cve: CVE-2021-26690
cve: CVE-2021-26691
cve: CVE-2021-30641
advisory_id: USN-4994-2
cert-bund: WID-SEC-2022-0438
cert-bund: WID-SEC-2022-0190
cert-bund: CB-K22/0072
cert-bund: CB-K21/1092
cert-bund: CB-K21/1090
cert-bund: CB-K21/0646
dfn-cert: DFN-CERT-2022-1047
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0098
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2365
dfn-cert: DFN-CERT-2021-2300
dfn-cert: DFN-CERT-2021-2187
dfn-cert: DFN-CERT-2021-2153
dfn-cert: DFN-CERT-2021-1467
dfn-cert: DFN-CERT-2021-1412
dfn-cert: DFN-CERT-2021-1355
dfn-cert: DFN-CERT-2021-1340
dfn-cert: DFN-CERT-2021-1333
dfn-cert: DFN-CERT-2021-1321
dfn-cert: DFN-CERT-2021-1317
dfn-cert: DFN-CERT-2021-1273
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5570-1)

Summary
The remote host is missing an update for the 'zlib' package(s) announced via the USN-5570-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   zlib1g
Installed version:    zlib1g-1:1.2.8.dfsg-1ubuntu1.1
Fixed version:      >=zlib1g-1:1.2.8.dfsg-1ubuntu1.1+esm2
```

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

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

Vulnerability Insight
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
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5570-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5570.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5570-1
cve: CVE-2022-37434
advisory_id: USN-5570-1
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-1438
cert-bund: WID-SEC-2022-0929
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-4129-2)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-4129-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm3
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm3
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm3
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

USN-4129-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM.
Original advisory details:
Thomas Vegas discovered that curl incorrectly handled memory during TFTP transfers. A remote attacker could use this issue to crash curl, 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-4129-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4129.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4129-2
cve: CVE-2019-5482
advisory_id: USN-4129-2
cert-bund: WID-SEC-2023-1637
cert-bund: WID-SEC-2023-1049
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/1016
cert-bund: CB-K20/0318
cert-bund: CB-K19/0809
dfn-cert: DFN-CERT-2021-0572
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2286
dfn-cert: DFN-CERT-2020-1898
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0555
dfn-cert: DFN-CERT-2020-0390
dfn-cert: DFN-CERT-2019-1906
dfn-cert: DFN-CERT-2019-1881
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4704-1)

Summary
The remote host is missing an update for the 'libsndfile' package(s) announced via the USN-4704-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsndfile1
Installed version:    libsndfile1-1.0.25-7ubuntu2.2
Fixed version:      >=libsndfile1-1.0.25-7ubuntu2.2+esm1
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'libsndfile' package(s) on Ubuntu 14.04, Ubuntu 16.04.

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. (CVE-2017-12562)
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. This issue only affected Ubuntu 14.04 ESM. (CVE-2017-14245, CVE-2017-14246, CVE-2017-14634, CVE-2017-16942, CVE-2017-6892, CVE-2018-13139, CVE-2018-19432, CVE-2018-19661, CVE-2018-19662, CVE-2018-19758, CVE-2019-3832)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4704-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4704.1
Version used: `2022-12-05T04:10:32Z`

References

```
url: https://ubuntu.com/security/notices/USN-4704-1
cve: CVE-2017-12562
cve: CVE-2017-14245
cve: CVE-2017-14246
cve: CVE-2017-14634
cve: CVE-2017-16942
cve: CVE-2017-6892
cve: CVE-2018-13139
cve: CVE-2018-19432
cve: CVE-2018-19661
cve: CVE-2018-19662
cve: CVE-2018-19758
cve: CVE-2019-3832
advisory_id: USN-4704-1
cert-bund: CB-K20/1030
cert-bund: CB-K18/0825
cert-bund: CB-K18/0216
cert-bund: CB-K17/1434
cert-bund: CB-K17/1051
dfn-cert: DFN-CERT-2022-1442
dfn-cert: DFN-CERT-2021-1667
dfn-cert: DFN-CERT-2021-0175
dfn-cert: DFN-CERT-2020-2352
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0899
dfn-cert: DFN-CERT-2020-0679
dfn-cert: DFN-CERT-2019-1158
dfn-cert: DFN-CERT-2019-0670
dfn-cert: DFN-CERT-2019-0074
dfn-cert: DFN-CERT-2018-2609
dfn-cert: DFN-CERT-2018-2563
dfn-cert: DFN-CERT-2018-1477
dfn-cert: DFN-CERT-2018-0233
dfn-cert: DFN-CERT-2017-1496
dfn-cert: DFN-CERT-2017-1072
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4019-2)

Summary
The remote host is missing an update for the 'sqlite3' package(s) announced via the USN-4019-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsqlite3-0
Installed version:    libsqlite3-0-3.8.2-1ubuntu2.2
Fixed version:      >=libsqlite3-0-3.8.2-1ubuntu2.2+esm1
```

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

Affected Software/OS
'sqlite3' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4019-1 fixed several vulnerabilities in sqlite3. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM.
Original advisory details:
It was discovered that SQLite incorrectly handled certain SQL files. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. (CVE-2017-2518)
It was discovered that SQLite incorrectly handled certain queries. An attacker could possibly use this issue to execute arbitrary code. (CVE-2018-20346, CVE-2018-20506)
It was discovered that SQLite incorrectly handled certain inputs. An attacker could possibly use this issue to access sensitive information. (CVE-2019-8457)
It was discovered that SQLite incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. (CVE-2016-6153)
It was discovered that SQLite incorrectly handled certain databases. An attacker could possibly use this issue to access sensitive information. This issue only affected Ubuntu 14.04 LTS. (CVE-2017-10989)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that SQLite incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-13685)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4019-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4019.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4019-2
cve: CVE-2016-6153
cve: CVE-2017-10989
cve: CVE-2017-13685
cve: CVE-2017-2518
cve: CVE-2018-20346
cve: CVE-2018-20506
cve: CVE-2019-8457
advisory_id: USN-4019-2
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-0582
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/0988
cert-bund: CB-K20/0287
cert-bund: CB-K20/0038
cert-bund: CB-K19/0915
cert-bund: CB-K19/0186
cert-bund: CB-K19/0086
cert-bund: CB-K19/0074
cert-bund: CB-K19/0073
cert-bund: CB-K17/1622
cert-bund: CB-K17/1585
cert-bund: CB-K17/1150
cert-bund: CB-K17/0827
cert-bund: CB-K17/0822
cert-bund: CB-K17/0492
cert-bund: CB-K16/1051
dfn-cert: DFN-CERT-2023-1179
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2005
dfn-cert: DFN-CERT-2020-2252
dfn-cert: DFN-CERT-2020-1840
dfn-cert: DFN-CERT-2020-1528
dfn-cert: DFN-CERT-2020-1325
dfn-cert: DFN-CERT-2020-0890
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0710
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2019-2486
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1248
dfn-cert: DFN-CERT-2019-1211
dfn-cert: DFN-CERT-2019-1125
dfn-cert: DFN-CERT-2019-0944
dfn-cert: DFN-CERT-2019-0811
dfn-cert: DFN-CERT-2019-0797
dfn-cert: DFN-CERT-2019-0794
dfn-cert: DFN-CERT-2019-0531
dfn-cert: DFN-CERT-2019-0454
dfn-cert: DFN-CERT-2019-0278
dfn-cert: DFN-CERT-2019-0171
dfn-cert: DFN-CERT-2019-0153
dfn-cert: DFN-CERT-2019-0151
dfn-cert: DFN-CERT-2019-0150
dfn-cert: DFN-CERT-2019-0084
dfn-cert: DFN-CERT-2019-0060
dfn-cert: DFN-CERT-2018-2569
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2018-1045
dfn-cert: DFN-CERT-2017-1692
dfn-cert: DFN-CERT-2017-1655
dfn-cert: DFN-CERT-2017-1188
dfn-cert: DFN-CERT-2017-0847
dfn-cert: DFN-CERT-2017-0846
dfn-cert: DFN-CERT-2017-0508
dfn-cert: DFN-CERT-2016-1115
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4038-2)

Summary
The remote host is missing an update for the 'bzip2' package(s) announced via the USN-4038-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   bzip2
Installed version:    bzip2-1.0.6-5
Fixed version:      >=bzip2-1.0.6-5ubuntu0.1~esm1
Vulnerable package:   libbz2-1.0
Installed version:    libbz2-1.0-1.0.6-5
Fixed version:      >=libbz2-1.0-1.0.6-5ubuntu0.1~esm1
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'bzip2' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4038-1 fixed several vulnerabilities in bzip2. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Aladdin Mubaied discovered that bzip2 incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2016-3189)
It was discovered that bzip2 incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-12900)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4038-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4038.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4038-2
cve: CVE-2016-3189
cve: CVE-2019-12900
advisory_id: USN-4038-2
cert-bund: WID-SEC-2023-1614
cert-bund: CB-K20/1021
cert-bund: CB-K19/0869
cert-bund: CB-K19/0536
cert-bund: CB-K17/0005
cert-bund: CB-K16/1102
dfn-cert: DFN-CERT-2022-0625
dfn-cert: DFN-CERT-2021-1418
dfn-cert: DFN-CERT-2020-2693
dfn-cert: DFN-CERT-2020-2287
dfn-cert: DFN-CERT-2019-1951
dfn-cert: DFN-CERT-2019-1775
dfn-cert: DFN-CERT-2019-1604
dfn-cert: DFN-CERT-2019-1497
dfn-cert: DFN-CERT-2019-1287
dfn-cert: DFN-CERT-2017-0002
dfn-cert: DFN-CERT-2016-1168
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4966-2)

Summary
The remote host is missing an update for the 'libx11' package(s) announced via the USN-4966-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libx11-6
Installed version:    libx11-6-2:1.6.2-1ubuntu2.1
Fixed version:      >=libx11-6-2:1.6.2-1ubuntu2.1+esm2
```

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

Affected Software/OS
'libx11' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-4966-1 fixed a vulnerability in libx11. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
It was discovered that libx11 incorrectly validated certain parameter lengths. A remote attacker could possibly use this issue to trick libx11 into emitting extra X protocol requests.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4966-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4966.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4966-2
cve: CVE-2021-31535
advisory_id: USN-4966-2
cert-bund: WID-SEC-2023-0063
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1905
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1123
dfn-cert: DFN-CERT-2021-1062
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

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

Vulnerability Detection Result

```
Vulnerable package:   klibc-utils
Installed version:    klibc-utils-2.0.3-0ubuntu1
Fixed version:      >=klibc-utils-2.0.3-0ubuntu1.14.04.3+esm2
Vulnerable package:   libklibc
Installed version:    libklibc-2.0.3-0ubuntu1
Fixed version:      >=libklibc-2.0.3-0ubuntu1.14.04.3+esm2
```

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)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5379.1

Version used: `2022-09-13T14:14:11Z`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1394
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-4231-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4231-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm4
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that NSS 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-4231-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4231.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4231-1
cve: CVE-2019-17006
advisory_id: USN-4231-1
cert-bund: WID-SEC-2022-1827
cert-bund: CB-K20/1030
cert-bund: CB-K20/0013
dfn-cert: DFN-CERT-2021-1111
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0573
dfn-cert: DFN-CERT-2021-0495
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2191
dfn-cert: DFN-CERT-2020-2137
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1697
dfn-cert: DFN-CERT-2020-1566
dfn-cert: DFN-CERT-2020-1450
dfn-cert: DFN-CERT-2020-1437
dfn-cert: DFN-CERT-2020-1316
dfn-cert: DFN-CERT-2020-0013
dfn-cert: DFN-CERT-2020-0001
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5810-4)

Summary
The remote host is missing an update for the 'git' package(s) announced via the USN-5810-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   git
Installed version:    git-1:1.9.1-1ubuntu0.10
Fixed version:      >=git-1:1.9.1-1ubuntu0.10+esm1
```

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

Affected Software/OS
'git' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-5810-1 fixed several vulnerabilities in Git. This update provides the corresponding update for Ubuntu 14.04 ESM.
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-5810-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5810.4
Version used: `2023-03-02T04:10:54Z`

References
`url: https://ubuntu.com/security/notices/USN-5810-4`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-23521
cve: CVE-2022-41903
advisory_id: USN-5810-4
cert-bund: WID-SEC-2023-1424
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-5254-1)

Summary
The remote host is missing an update for the 'shadow' package(s) announced via the USN-5254-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   login
Installed version:    login-1:4.1.5.1-1ubuntu9.5
Fixed version:      >=login-1:4.1.5.1-1ubuntu9.5+esm1
Vulnerable package:   passwd
Installed version:    passwd-1:4.1.5.1-1ubuntu9.5
Fixed version:      >=passwd-1:4.1.5.1-1ubuntu9.5+esm1
```

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.

Vulnerability Insight
It was discovered that shadow incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or expose sensitive information. This issue only affected Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. (CVE-2017-12424)
It was discovered that shadow incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. (CVE-2018-7169)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5254-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5254.1
Version used: `2022-09-13T14:14:11Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-5254-1
cve: CVE-2017-12424
cve: CVE-2018-7169
advisory_id: USN-5254-1
cert-bund: CB-K18/0448
cert-bund: CB-K17/1903
dfn-cert: DFN-CERT-2022-0206
dfn-cert: DFN-CERT-2021-0568
dfn-cert: DFN-CERT-2018-0474
dfn-cert: DFN-CERT-2017-1982
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5487-3)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5487-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm8
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm8
```

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.

Vulnerability Insight
USN-5487-1 fixed several vulnerabilities in Apache HTTP Server. Unfortunately it caused regressions. USN-5487-2 reverted the patches that caused the regression in Ubuntu 14.04 ESM for further investigation. This update re-adds the security fixes for Ubuntu 14.04 ESM and fixes two different regressions: one affecting mod_proxy only in Ubuntu 14.04 ESM and another in mod_sed affecting also Ubuntu 16.04 ESM and Ubuntu 18.04 LTS.
We apologize for the inconvenience.
Original advisory details:
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-5487-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5487.3
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5487-3
url: https://launchpad.net/bugs/1979577
url: https://launchpad.net/bugs/1979641
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-5487-3
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
dfn-cert: DFN-CERT-2022-2167
dfn-cert: DFN-CERT-2022-1837
dfn-cert: DFN-CERT-2022-1833
dfn-cert: DFN-CERT-2022-1720
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1353
dfn-cert: DFN-CERT-2022-1296
```

High (CVSS: 9.8)
NVT: Ubuntu: Security Advisory (USN-5487-2)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5487-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm6
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm6
```

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

Affected Software/OS
'apache2' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-5487-1 fixed several vulnerabilities in Apache. Unfortunately, that update introduced a regression when proxying balancer manager connections in some configurations on Ubuntu 14.04 ESM. This update reverts those changes till further fix.
We apologize for the inconvenience.
Original advisory details:
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-5487-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5487.2
Version used: `2022-09-16T08:45:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5487-2
url: https://launchpad.net/bugs/1979577
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-5487-2
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
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-5487-1)

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-5487-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm5
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm5
```

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

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: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5487-1
cve: CVE-2022-26377
cve: CVE-2022-28614
```

... continues on next page ...

. . . continued from previous page . . .

```
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-2023-0134
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
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-5168-3)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5168-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm9
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 14.04, Ubuntu 16.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-5168-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Original advisory details:

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-5168-3)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.5168.3

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5168-3
cve: CVE-2021-43527
advisory_id: USN-5168-3
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-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-5168-4)

Summary

The remote host is missing an update for the ’nss’ package(s) announced via the USN-5168-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm10
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5168-3 fixed a vulnerability in NSS. Unfortunately that update introduced a regression that could break SSL connections. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
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-5168-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5168.4
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5168-4
cve: CVE-2021-43527
advisory_id: USN-5168-4
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-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-5702-2)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5702-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm13
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm13
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm13
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5702-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5702-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5702.2
Version used: `2022-12-12T04:10:32Z`

References

```
url: https://ubuntu.com/security/notices/USN-5702-2
cve: CVE-2022-32221
advisory_id: USN-5702-2
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
```

... continues on next page ...

... continued from previous page ...

```
cert-bund: WID-SEC-2023-0189
cert-bund: WID-SEC-2023-0126
cert-bund: WID-SEC-2022-2372
cert-bund: WID-SEC-2022-1862
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0372
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
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-5333-2)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5333-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm4
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm4
```

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

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

Vulnerability Insight
USN-5333-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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)

... continues on next page ...

. . . continued from previous page . . .

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-5333-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5333.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5333-2
cve: CVE-2022-22719
cve: CVE-2022-22720
cve: CVE-2022-22721
cve: CVE-2022-23943
advisory_id: USN-5333-2
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-5212-2)

Summary
The remote host is missing an update for the 'apache2' package(s) announced via the USN-5212-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm3
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm3
```

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

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

Vulnerability Insight
USN-5212-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5212-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5212.2
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-5212-2`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2021-44224
cve: CVE-2021-44790
advisory_id: USN-5212-2
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-5825-1)

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

Vulnerability Detection Result

```
Vulnerable package:   libpam-modules
Installed version:    libpam-modules-1.1.8-1ubuntu2.2
Fixed version:      >=libpam-modules-1.1.8-1ubuntu2.2+esm1
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2023-01-26T04:10:44Z`

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-5090-2)

Summary

The remote host is missing an update for the 'apache2' package(s) announced via the USN-5090-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apache2
Installed version:    apache2-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-2.4.7-1ubuntu4.22+esm2
Vulnerable package:   apache2-bin
Installed version:    apache2-bin-2.4.7-1ubuntu4.22
Fixed version:      >=apache2-bin-2.4.7-1ubuntu4.22+esm2
```

Solution:

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

Affected Software/OS

'apache2' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

USN-5090-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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 . . .

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-5090-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5090.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5090-2
cve: CVE-2021-34798
cve: CVE-2021-39275
cve: CVE-2021-40438
advisory_id: USN-5090-2
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-2022-0190
cert-bund: CB-K22/0476
cert-bund: CB-K22/0465
cert-bund: CB-K22/0463
cert-bund: CB-K21/0992
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2022-2405
dfn-cert: DFN-CERT-2022-2167
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-2047
dfn-cert: DFN-CERT-2021-2020
dfn-cert: DFN-CERT-2021-1961
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-4991-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-4991-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.1+dfsg1-3ubuntu4.13
Fixed version:      >=libxml2-2.9.1+dfsg1-3ubuntu4.13+esm2
```

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 20.10, Ubuntu 21.04.

Vulnerability Insight
Yunho Kim discovered that libxml2 incorrectly handled certain error conditions. A remote attacker could exploit this with a crafted XML file to cause a denial of service, or possibly cause libxml2 to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, and Ubuntu 16.04 ESM. (CVE-2017-8872)
Zhipeng Xie discovered that libxml2 incorrectly handled certain XML schemas. A remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. (CVE-2019-20388)
It was discovered that libxml2 incorrectly handled invalid UTF-8 input. A remote attacker could possibly exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 20.10. (CVE-2020-24977)
It was discovered that libxml2 incorrectly handled invalid UTF-8 input. A remote attacker could possibly exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. (CVE-2021-3517)
It was discovered that libxml2 did not properly handle certain crafted XML files. A local attacker could exploit this with a crafted input to cause libxml2 to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-3516, CVE-2021-3518)
It was discovered that libxml2 incorrectly handled error states. A remote attacker could exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. (CVE-2021-3537)

. . . continues on next page . . .

. . . continued from previous page . . .

Sebastian Pipping discovered that libxml2 did not properly handle certain crafted XML files. A remote attacker could exploit this with a crafted XML file to cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. (CVE-2021-3541)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4991-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4991.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4991-1
cve: CVE-2017-8872
cve: CVE-2019-20388
cve: CVE-2020-24977
cve: CVE-2021-3516
cve: CVE-2021-3517
cve: CVE-2021-3518
cve: CVE-2021-3537
cve: CVE-2021-3541
advisory_id: USN-4991-1
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1153
cert-bund: WID-SEC-2023-1152
cert-bund: WID-SEC-2023-1151
cert-bund: WID-SEC-2023-0395
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1772
cert-bund: WID-SEC-2022-1051
cert-bund: WID-SEC-2022-0196
cert-bund: WID-SEC-2022-0094
cert-bund: CB-K22/0476
cert-bund: CB-K22/0466
cert-bund: CB-K22/0061
cert-bund: CB-K21/1092
cert-bund: CB-K21/1087
cert-bund: CB-K21/1082
cert-bund: CB-K21/0794
cert-bund: CB-K21/0792
cert-bund: CB-K21/0648
cert-bund: CB-K21/0494
cert-bund: CB-K21/0450
cert-bund: CB-K20/1030
cert-bund: CB-K20/0867
cert-bund: CB-K20/0708
cert-bund: CB-K18/0157
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1709
cert-bund: CB-K17/1563
cert-bund: CB-K17/1348
dfn-cert: DFN-CERT-2023-0969
dfn-cert: DFN-CERT-2022-2305
dfn-cert: DFN-CERT-2022-1875
dfn-cert: DFN-CERT-2022-0899
dfn-cert: DFN-CERT-2022-0879
dfn-cert: DFN-CERT-2022-0872
dfn-cert: DFN-CERT-2022-0213
dfn-cert: DFN-CERT-2022-0121
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2195
dfn-cert: DFN-CERT-2021-2188
dfn-cert: DFN-CERT-2021-1802
dfn-cert: DFN-CERT-2021-1690
dfn-cert: DFN-CERT-2021-1577
dfn-cert: DFN-CERT-2021-1576
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1168
dfn-cert: DFN-CERT-2021-1102
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-1049
dfn-cert: DFN-CERT-2021-0989
dfn-cert: DFN-CERT-2021-0982
dfn-cert: DFN-CERT-2021-0969
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-1989
dfn-cert: DFN-CERT-2020-1986
dfn-cert: DFN-CERT-2020-1974
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2020-0753
dfn-cert: DFN-CERT-2020-0312
dfn-cert: DFN-CERT-2018-0169
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1630
dfn-cert: DFN-CERT-2017-1408
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-4277-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'libexif' package(s) announced via the USN-4277-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexif12
Installed version:    libexif12-0.6.21-1ubuntu1
Fixed version:      >=libexif12-0.6.21-1ubuntu1+esm1
```

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

Affected Software/OS
'libexif' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
Liu Bingchang discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information or cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2016-6328)
Lili Xu and Bingchang Liu discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information or cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2017-7544)
It was discovered that libexif incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-9278)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4277-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4277.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4277-1
cve: CVE-2016-6328
cve: CVE-2017-7544
cve: CVE-2019-9278
advisory_id: USN-4277-1
cert-bund: WID-SEC-2022-1994
cert-bund: CB-K21/0007
cert-bund: CB-K20/1030
cert-bund: CB-K20/0107
cert-bund: CB-K19/0757
cert-bund: CB-K18/0158
cert-bund: CB-K17/2195
dfn-cert: DFN-CERT-2021-0162
dfn-cert: DFN-CERT-2021-0010
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2400
dfn-cert: DFN-CERT-2020-2135
dfn-cert: DFN-CERT-2020-1190
dfn-cert: DFN-CERT-2020-1174
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-1050
dfn-cert: DFN-CERT-2020-0393
dfn-cert: DFN-CERT-2020-0308
dfn-cert: DFN-CERT-2020-0301
dfn-cert: DFN-CERT-2020-0273
dfn-cert: DFN-CERT-2018-0175
dfn-cert: DFN-CERT-2017-2294
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-4396-1)

Summary
The remote host is missing an update for the 'libexif' package(s) announced via the USN-4396-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexif12
Installed version:    libexif12-0.6.21-1ubuntu1
Fixed version:      >=libexif12-0.6.21-1ubuntu1+esm5
```

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

Affected Software/OS
'libexif' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-0093, CVE-2020-0182)
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a remote denial of service. (CVE-2020-0198)
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information or cause a crash. (CVE-2020-13112)
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. (CVE-2020-13113)
It was discovered libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-13114)

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-4396-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4396.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4396-1
cve: CVE-2020-0093
cve: CVE-2020-0182
cve: CVE-2020-0198
cve: CVE-2020-13112
cve: CVE-2020-13113
cve: CVE-2020-13114
advisory_id: USN-4396-1
cert-bund: CB-K22/0149
cert-bund: CB-K20/1030
cert-bund: CB-K20/0517
cert-bund: CB-K20/0491
cert-bund: CB-K20/0421
dfn-cert: DFN-CERT-2022-0287
dfn-cert: DFN-CERT-2020-2455
dfn-cert: DFN-CERT-2020-2400
dfn-cert: DFN-CERT-2020-2135
dfn-cert: DFN-CERT-2020-1325
dfn-cert: DFN-CERT-2020-1285
dfn-cert: DFN-CERT-2020-1273
dfn-cert: DFN-CERT-2020-1262
dfn-cert: DFN-CERT-2020-1190
dfn-cert: DFN-CERT-2020-1174
dfn-cert: DFN-CERT-2020-1151
dfn-cert: DFN-CERT-2020-1132
dfn-cert: DFN-CERT-2020-1050
dfn-cert: DFN-CERT-2020-0937
```

High (CVSS: 9.1)
NVT: Ubuntu: Security Advisory (USN-4476-1)

Summary

The remote host is missing an update for the 'nss' package(s) announced via the USN-4476-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm8
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that NSS incorrectly handled some inputs. 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-4476-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4476.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4476-1
cve: CVE-2020-12403
advisory_id: USN-4476-1
cert-bund: WID-SEC-2022-1831
cert-bund: CB-K20/1030
dfn-cert: DFN-CERT-2023-0411
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0573
dfn-cert: DFN-CERT-2021-0495
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2137
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1872
dfn-cert: DFN-CERT-2020-1646
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5553-1)

Summary
The remote host is missing an update for the 'libjpeg-turbo' package(s) announced via the USN-5553-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjpeg-turbo8
Installed version:    libjpeg-turbo8-1.3.0-0ubuntu2.1
Fixed version:      >=libjpeg-turbo8-1.3.0-0ubuntu2.1+esm2
```

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Please install the updated package(s).

Affected Software/OS
'libjpeg-turbo' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that libjpeg-turbo was not properly handling EOF characters, which could lead to excessive memory consumption through the execution of a large loop. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-11813)
It was discovered that libjpeg-turbo was not properly performing bounds check operations, which could lead to a heap-based buffer overread. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM. (CVE-2018-14498)
It was discovered that libjpeg-turbo was not properly limiting the amount of main memory being consumed by the system during decompression or multi-pass compression operations, which could lead to excessive memory consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-14152)
It was discovered that libjpeg-turbo was not properly setting variable sizes when performing certain kinds of encoding operations, which could lead to a stack-based buffer overflow. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service. (CVE-2020-17541)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5553-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5553.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5553-1
cve: CVE-2018-11813
cve: CVE-2018-14498
cve: CVE-2020-14152
cve: CVE-2020-17541
advisory_id: USN-5553-1
cert-bund: WID-SEC-2022-0571
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K21/1164
cert-bund: CB-K20/1049
cert-bund: CB-K19/0696
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-2020-1682
dfn-cert: DFN-CERT-2019-2394
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1615
dfn-cert: DFN-CERT-2019-1105
dfn-cert: DFN-CERT-2019-0590
dfn-cert: DFN-CERT-2019-0520
dfn-cert: DFN-CERT-2018-1243
dfn-cert: DFN-CERT-2018-1168
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-4126-2)

Summary
The remote host is missing an update for the 'freetype' package(s) announced via the USN-4126-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libfreetype6
Installed version:    libfreetype6-2.5.2-1ubuntu2.8
Fixed version:      >=libfreetype6-2.5.2-1ubuntu2.8+esm1
```

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

Affected Software/OS
'freetype' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4126-1 fixed a vulnerability in FreeType. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
It was discovered that FreeType incorrectly handled certain font files. An attacker could possibly use this issue to access sensitive information. (CVE-2015-9381, CVE-2015-9382)
Original advisory details:
It was discovered that FreeType incorrectly handled certain font files. An attacker could possibly use this issue to access sensitive information. (CVE-2015-9383)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4126-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4126.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4126-2
cve: CVE-2015-9381
cve: CVE-2015-9382
cve: CVE-2015-9383
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-4126-2
cert-bund: CB-K19/1086
dfn-cert: DFN-CERT-2021-0095
dfn-cert: DFN-CERT-2019-1842
dfn-cert: DFN-CERT-2019-1457
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-4305-1)

Summary
The remote host is missing an update for the 'icu' package(s) announced via the USN-4305-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libicu52
Installed version:    libicu52-52.1-3ubuntu0.8
Fixed version:      >=libicu52-52.1-3ubuntu0.8+esm1
```

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

Affected Software/OS
'icu' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
Andre Bargull discovered that ICU incorrectly handled certain strings. 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-4305-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4305.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4305-1
cve: CVE-2020-10531
advisory_id: USN-4305-1
cert-bund: WID-SEC-2023-1374
cert-bund: WID-SEC-2022-1077
cert-bund: WID-SEC-2022-0075
cert-bund: CB-K20/1049
cert-bund: CB-K20/1015
cert-bund: CB-K20/0544
cert-bund: CB-K20/0241
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2303
dfn-cert: DFN-CERT-2020-1962
dfn-cert: DFN-CERT-2020-1501
dfn-cert: DFN-CERT-2020-1164
dfn-cert: DFN-CERT-2020-0559
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libgssapi-krb5-2
Installed version:    libgssapi-krb5-2-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libgssapi-krb5-2-1.12+dfsg-2ubuntu5.4+esm3
Vulnerable package:   libkdb5-7
Installed version:    libkdb5-7-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkdb5-7-1.12+dfsg-2ubuntu5.4+esm3
```

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: `2023-01-26T04:10:44Z`

References

```
url: https://ubuntu.com/security/notices/USN-5828-1
cve: CVE-2018-20217
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2022-42898
advisory_id: USN-5828-1
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-2023-1592
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-4154-1)

Summary
The remote host is missing an update for the 'sudo' package(s) announced via the USN-4154-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm2
```

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

Affected Software/OS
'sudo' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Joe Vennix discovered that Sudo incorrectly handled certain user IDs. An attacker could potentially exploit this to execute arbitrary commands as the root user.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4154-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4154.1
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4154-1
cve: CVE-2019-14287
advisory_id: USN-4154-1
cert-bund: CB-K19/0902
dfn-cert: DFN-CERT-2019-2461
dfn-cert: DFN-CERT-2019-2445
dfn-cert: DFN-CERT-2019-2444
dfn-cert: DFN-CERT-2019-2136
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5260-3)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-5260-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm12
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5260-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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)

. . . 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-5260-3)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5260.3

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5260-3
cve: CVE-2021-44142
advisory_id: USN-5260-3
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
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
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-3655-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-3655-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.149.159
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

Jann Horn and Ken Johnson discovered that microprocessors utilizing speculative execution of a memory read may allow unauthorized memory reads via a sidechannel attack. This flaw is known as Spectre Variant 4. A local attacker could use this to expose sensitive information, including kernel memory. (CVE-2018-3639)
Jan H. Schonherr discovered that the Xen subsystem did not properly handle block IO merges correctly in some situations. An attacker in a guest vm could use this to cause a denial of service (host crash) or possibly gain administrative privileges in the host. (CVE-2017-12134)
It was discovered that the Bluetooth HIP Protocol implementation in the Linux kernel did not properly validate HID connection setup information. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-13220)
It was discovered that a buffer overread vulnerability existed in the keyring subsystem of the Linux kernel. A local attacker could possibly use this to expose sensitive information (kernel memory). (CVE-2017-13305)
It was discovered that the netlink subsystem in the Linux kernel did not properly restrict observations of netlink messages to the appropriate net namespace. A local attacker could use this to expose sensitive information (kernel netlink traffic). (CVE-2017-17449)
It was discovered that a race condition existed in the i8042 serial device driver implementation in the Linux kernel. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-18079)
It was discovered that a race condition existed in the Device Mapper component of the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-18203)
It was discovered that a race condition existed in the OCFS2 file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (kernel deadlock). (CVE-2017-18204)
It was discovered that an infinite loop could occur in the madvise(2) implementation in the Linux kernel in certain circumstances. A local attacker could use this to cause a denial of service (system hang). (CVE-2017-18208)
Kefeng Wang discovered that a race condition existed in the memory locking implementation in the Linux kernel. A local attacker could use this to cause a denial of service. (CVE-2017-18221)
Silvio Cesare discovered a buffer overwrite existed in the NCPFS implementation in the Linux kernel. A remote attacker controlling a malicious NCPFS server could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-8822)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3655-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3655.1
Version used: `2023-03-06T04:11:16Z`

References

```
url: https://ubuntu.com/security/notices/USN-3655-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/Variant4
cve: CVE-2017-12134
cve: CVE-2017-13220
cve: CVE-2017-13305
cve: CVE-2017-17449
```

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-18079
cve: CVE-2017-18203
cve: CVE-2017-18204
cve: CVE-2017-18208
cve: CVE-2017-18221
cve: CVE-2018-3639
cve: CVE-2018-8822
advisory_id: USN-3655-1
cert-bund: WID-SEC-2023-0531
cert-bund: WID-SEC-2023-0527
cert-bund: WID-SEC-2022-0532
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
cert-bund: CB-K18/0635
cert-bund: CB-K18/0557
cert-bund: CB-K18/0550
cert-bund: CB-K18/0523
cert-bund: CB-K18/0367
cert-bund: CB-K18/0347
cert-bund: CB-K18/0184
cert-bund: CB-K18/0165
cert-bund: CB-K18/0080
cert-bund: CB-K18/0051
cert-bund: CB-K18/0040
cert-bund: CB-K18/0004
cert-bund: CB-K17/2223
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
cert-bund: CB-K17/2187
cert-bund: CB-K17/2141
cert-bund: CB-K17/2124
cert-bund: CB-K17/1908
cert-bund: CB-K17/1840
cert-bund: CB-K17/1813
cert-bund: CB-K17/1708
cert-bund: CB-K17/1607
cert-bund: CB-K17/1602
cert-bund: CB-K17/1567
cert-bund: CB-K17/1521
cert-bund: CB-K17/1442
cert-bund: CB-K17/1418
cert-bund: CB-K17/1379
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2020-2594
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2592
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-2019-2615
dfn-cert: DFN-CERT-2019-2552
dfn-cert: DFN-CERT-2019-2514
dfn-cert: DFN-CERT-2019-1673
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1008
dfn-cert: DFN-CERT-2019-0809
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0259
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0245
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-2019-0027
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2019-0020
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2393
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-2018-2206
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1767
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1658
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1627
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1374
dfn-cert: DFN-CERT-2018-1355
dfn-cert: DFN-CERT-2018-1353
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1323
dfn-cert: DFN-CERT-2018-1304
dfn-cert: DFN-CERT-2018-1279
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-2018-1190
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
dfn-cert: DFN-CERT-2018-0947
dfn-cert: DFN-CERT-2018-0932
dfn-cert: DFN-CERT-2018-0915
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0883
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0799
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0780
dfn-cert: DFN-CERT-2018-0775
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0737
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0605
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0560
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0095
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0008
dfn-cert: DFN-CERT-2017-2319
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2286
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1787
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1669
dfn-cert: DFN-CERT-2017-1637
dfn-cert: DFN-CERT-2017-1588
dfn-cert: DFN-CERT-2017-1501
dfn-cert: DFN-CERT-2017-1479
dfn-cert: DFN-CERT-2017-1441
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5378-3)

Summary
The remote host is missing an update for the 'xz-utils' package(s) announced via the USN-5378-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   xz-utils
Installed version:    xz-utils-5.1.1alpha+20120614-2ubuntu2
Fixed version:      >=xz-utils-5.1.1alpha+20120614-2ubuntu2.14.04.1+esm1
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'xz-utils' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5378-2 fixed a vulnerability in XZ Utils. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.
Original advisory details:
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-5378-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5378.3
Version used: `2022-09-16T08:45:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5378-3
cve: CVE-2022-1271
advisory_id: USN-5378-3
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-5575-2)

Summary
The remote host is missing an update for the 'libxslt' package(s) announced via the USN-5575-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxslt1.1
Installed version:    libxslt1.1-1.1.28-2ubuntu0.2
Fixed version:      >=libxslt1.1-1.1.28-2ubuntu0.2+esm2
```

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

Affected Software/OS
'libxslt' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5575-1 fixed vulnerabilities in Libxslt. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5575-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5575.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5575-2
cve: CVE-2019-5815
cve: CVE-2021-30560
advisory_id: USN-5575-2
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-5841-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5841-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm6
```

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

Affected Software/OS
'tiff' package(s) on Ubuntu 14.04, Ubuntu 16.04.

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. This issue was only fixed in Ubuntu 14.04 ESM. (CVE-2019-14973, CVE-2019-17546, CVE-2020-35523, CVE-2020-35524, CVE-2022-3970)
It was discovered that LibTIFF was incorrectly acessing a data structure when processing data with the tiffcrop tool, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2022-48281)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5841-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5841.1
Version used: `2023-02-03T04:10:38Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-5841-1
cve: CVE-2019-14973
cve: CVE-2019-17546
cve: CVE-2020-35523
cve: CVE-2020-35524
cve: CVE-2022-3970
cve: CVE-2022-48281
advisory_id: USN-5841-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2023-0271
cert-bund: WID-SEC-2023-0270
cert-bund: WID-SEC-2023-0170
cert-bund: WID-SEC-2022-2035
cert-bund: WID-SEC-2022-0914
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0395
dfn-cert: DFN-CERT-2023-1445
dfn-cert: DFN-CERT-2023-1124
dfn-cert: DFN-CERT-2023-1050
dfn-cert: DFN-CERT-2023-0884
dfn-cert: DFN-CERT-2023-0220
dfn-cert: DFN-CERT-2023-0218
dfn-cert: DFN-CERT-2023-0141
dfn-cert: DFN-CERT-2023-0120
dfn-cert: DFN-CERT-2022-2695
dfn-cert: DFN-CERT-2022-2680
dfn-cert: DFN-CERT-2022-0395
dfn-cert: DFN-CERT-2022-0389
dfn-cert: DFN-CERT-2021-2371
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0702
dfn-cert: DFN-CERT-2021-0612
dfn-cert: DFN-CERT-2021-0433
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-0918
dfn-cert: DFN-CERT-2020-0340
dfn-cert: DFN-CERT-2020-0308
dfn-cert: DFN-CERT-2020-0146
dfn-cert: DFN-CERT-2019-2507
dfn-cert: DFN-CERT-2019-2495
dfn-cert: DFN-CERT-2019-1773
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-4298-2)

Summary
The remote host is missing an update for the 'sqlite3' package(s) announced via the USN-4298-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsqlite3-0
Installed version:    libsqlite3-0-3.8.2-1ubuntu2.2
Fixed version:      >=libsqlite3-0-3.8.2-1ubuntu2.2+esm2
```

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

Affected Software/OS
'sqlite3' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4298-1 fixed several vulnerabilities in SQLite. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that SQLite incorrectly handled certain shadow tables. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2019-13734, CVE-2019-13750, CVE-2019-13752, CVE-2019-13753)
It was discovered that SQLite incorrectly handled certain corrupt records. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2019-13751)
It was discovered that SQLite incorrectly handled errors during parsing. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2019-19926)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4298-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4298.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4298-2
cve: CVE-2019-13734
cve: CVE-2019-13750
cve: CVE-2019-13751
cve: CVE-2019-13752
cve: CVE-2019-13753
cve: CVE-2019-19926
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-4298-2
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1049
cert-bund: WID-SEC-2022-0624
cert-bund: CB-K20/1049
cert-bund: CB-K20/0845
cert-bund: CB-K20/0318
cert-bund: CB-K20/0157
cert-bund: CB-K20/0097
cert-bund: CB-K19/1058
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2356
dfn-cert: DFN-CERT-2021-2005
dfn-cert: DFN-CERT-2021-1501
dfn-cert: DFN-CERT-2020-2259
dfn-cert: DFN-CERT-2020-0890
dfn-cert: DFN-CERT-2020-0489
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2020-0317
dfn-cert: DFN-CERT-2020-0245
dfn-cert: DFN-CERT-2020-0179
dfn-cert: DFN-CERT-2019-2604
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5025-2)

Summary
The remote host is missing an update for the 'libsndfile' package(s) announced via the USN-5025-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsndfile1
Installed version:    libsndfile1-1.0.25-7ubuntu2.2
Fixed version:      >=libsndfile1-1.0.25-7ubuntu2.2+esm2
```

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

Affected Software/OS
'libsndfile' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5025-1 fixed a vulnerability in libsndfile. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

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-5025-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5025.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5025-2
cve: CVE-2021-3246
advisory_id: USN-5025-2
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-5718-2)

Summary

The remote host is missing an update for the 'pixman' package(s) announced via the USN-5718-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libpixman-1-0
Installed version:    libpixman-1-0-0.30.2-2ubuntu1.2
Fixed version:      >=libpixman-1-0-0.30.2-2ubuntu1.2+esm1
```

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

Affected Software/OS

'pixman' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

USN-5718-1 fixed a vulnerability in pixman. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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.

. . . 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-5718-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5718.2
Version used: `2022-12-01T04:11:08Z`

References

```
url: https://ubuntu.com/security/notices/USN-5718-2
cve: CVE-2022-44638
advisory_id: USN-5718-2
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-5892-2)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5892-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm12
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5892-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: Ubuntu: Security Advisory (USN-5892-2)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5892.2
Version used: 2023-06-12T04:09:28Z

References

```
url: https://ubuntu.com/security/notices/USN-5892-2
cve: CVE-2023-0767
advisory_id: USN-5892-2
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0407
cert-bund: WID-SEC-2023-0385
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-5964-2)

Summary

The remote host is missing an update for the 'curl' package(s) announced via the USN-5964-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm15
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm15
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm15
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'curl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

USN-5964-1 fixed several vulnerabilities in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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 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)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5964-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5964.2
Version used: `2023-06-02T04:09:24Z`

References
```
url: https://ubuntu.com/security/notices/USN-5964-2
cve: CVE-2023-27533
cve: CVE-2023-27535
cve: CVE-2023-27536
advisory_id: USN-5964-2
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0690
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-5872-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-5872-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm11
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 14.04, Ubuntu 16.04.

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. (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-5872-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5872.1
Version used: `2023-02-16T04:10:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-5872-1
cve: CVE-2022-22747
cve: CVE-2022-34480
advisory_id: USN-5872-1
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
dfn-cert: DFN-CERT-2022-0046
dfn-cert: DFN-CERT-2022-0045
```

High (CVSS: 8.8)
NVT: Ubuntu: Security Advisory (USN-5378-4)

Summary
The remote host is missing an update for the 'gzip' package(s) announced via the USN-5378-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   gzip
Installed version:    gzip-1.6-3ubuntu1
Fixed version:      >=gzip-1.6-3ubuntu1+esm1
```

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

Affected Software/OS
'gzip' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5378-1 fixed a vulnerability in Gzip. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.
Original advisory details:
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-5378-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5378.4
Version used: `2022-09-16T08:45:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5378-4
cve: CVE-2022-1271
advisory_id: USN-5378-4
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-4203-2)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4203-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm2
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4203-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was 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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4203-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4203.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4203-2
cve: CVE-2019-11745
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-4203-2
cert-bund: WID-SEC-2022-1826
cert-bund: CB-K19/1040
cert-bund: CB-K19/1038
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0095
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1450
dfn-cert: DFN-CERT-2020-1425
dfn-cert: DFN-CERT-2020-0666
dfn-cert: DFN-CERT-2020-0114
dfn-cert: DFN-CERT-2020-0103
dfn-cert: DFN-CERT-2020-0001
dfn-cert: DFN-CERT-2019-2609
dfn-cert: DFN-CERT-2019-2579
dfn-cert: DFN-CERT-2019-2566
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2557
dfn-cert: DFN-CERT-2019-2480
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libncurses5
Installed version:    libncurses5-5.9+20140118-1ubuntu1
Fixed version:      >=libncurses5-5.9+20140118-1ubuntu1+esm3
Vulnerable package:   libncursesw5
Installed version:    libncursesw5-5.9+20140118-1ubuntu1
Fixed version:      >=libncursesw5-5.9+20140118-1ubuntu1+esm3
Vulnerable package:   libtinfo5
Installed version:    libtinfo5-5.9+20140118-1ubuntu1
Fixed version:      >=libtinfo5-5.9+20140118-1ubuntu1+esm3
Vulnerable package:   ncurses-bin
Installed version:    ncurses-bin-5.9+20140118-1ubuntu1
Fixed version:      >=ncurses-bin-5.9+20140118-1ubuntu1+esm3
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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.
Details: `Ubuntu: Security Advisory (USN-6099-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6099.1
Version used: `2023-05-24T04:09:15Z`

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-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-2023-1186
dfn-cert: DFN-CERT-2023-1033
dfn-cert: DFN-CERT-2022-2601
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-5477-1)

Summary
The remote host is missing an update for the 'ncurses' package(s) announced via the USN-5477-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libncurses5
Installed version:    libncurses5-5.9+20140118-1ubuntu1
Fixed version:      >=libncurses5-5.9+20140118-1ubuntu1+esm2
Vulnerable package:   libtinfo5
Installed version:    libtinfo5-5.9+20140118-1ubuntu1
Fixed version:      >=libtinfo5-5.9+20140118-1ubuntu1+esm2
Vulnerable package:   ncurses-bin
Installed version:    ncurses-bin-5.9+20140118-1ubuntu1
Fixed version:      >=ncurses-bin-5.9+20140118-1ubuntu1+esm2
```

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

Affected Software/OS
'ncurses' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
Hosein Askari discovered that ncurses was incorrectly performing memory management operations when dealing with long filenames while writing structures into the file system. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2017-16879)
Chung-Yi Lin discovered that ncurses was incorrectly handling access to invalid memory areas when parsing terminfo or termcap entries where the use-name had invalid syntax. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-19211)
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. (CVE-2019-17594)

. . . continues on next page . . .

... continued from previous page ...

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. (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. (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. (CVE-2022-29458)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5477-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5477.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5477-1
cve: CVE-2017-16879
cve: CVE-2018-19211
cve: CVE-2019-17594
cve: CVE-2019-17595
cve: CVE-2021-39537
cve: CVE-2022-29458
advisory_id: USN-5477-1
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
cert-bund: CB-K17/2095
dfn-cert: DFN-CERT-2023-1186
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
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2018-2486
dfn-cert: DFN-CERT-2017-2190
```

High (CVSS: 8.6)
NVT: Ubuntu: Security Advisory (USN-4602-2)

Summary
The remote host is missing an update for the 'perl' package(s) announced via the USN-4602-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   perl
Installed version:    perl-5.18.2-2ubuntu1.7
Fixed version:      >=perl-5.18.2-2ubuntu1.7+esm3
```

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

Affected Software/OS
'perl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4602-1 fixed several vulnerabilities in Perl. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
ManhND discovered that Perl incorrectly handled certain regular expressions. In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-10543)
Hugo van der Sanden and Slaven Rezic discovered that Perl incorrectly handled certain regular expressions. In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-10878)
Sergey Aleynikov discovered that Perl incorrectly handled certain regular expressions. In environments where untrusted regular expressions are evaluated, a remote attacker could possibly use this issue to cause Perl to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-12723)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4602-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4602.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4602-2
cve: CVE-2020-10543
cve: CVE-2020-10878
cve: CVE-2020-12723
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-4602-2
cert-bund: WID-SEC-2023-1319
cert-bund: WID-SEC-2022-1910
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1767
cert-bund: WID-SEC-2022-0624
cert-bund: WID-SEC-2022-0623
cert-bund: CB-K21/0788
cert-bund: CB-K20/1228
cert-bund: CB-K20/0546
dfn-cert: DFN-CERT-2021-1561
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0358
dfn-cert: DFN-CERT-2020-1156
```

High (CVSS: 8.4)
NVT: Ubuntu: Security Advisory (USN-3822-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3822-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.162.172
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Jim Mattson discovered that the KVM implementation in the Linux kernel mismanages the #BP and #OF exceptions. A local attacker in a guest virtual machine could use this to cause a denial of service (guest OS crash). (CVE-2016-9588)
It was discovered that the generic SCSI driver in the Linux kernel did not properly enforce permissions on kernel memory access. A local attacker could use this to expose sensitive information or possibly elevate privileges. (CVE-2017-13168)
Andrey Konovalov discovered that the CDC USB Ethernet driver did not properly validate device descriptors. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2017-16649)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that an integer overflow existed in the CD-ROM driver of the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2018-16658)
It was discovered that an integer overflow existed in the HID Bluetooth implementation in the Linux kernel that could lead to a buffer overwrite. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-9363)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3822-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3822.1
Version used: `2023-01-23T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-3822-1
cve: CVE-2016-9588
cve: CVE-2017-13168
cve: CVE-2017-16649
cve: CVE-2018-16658
cve: CVE-2018-9363
advisory_id: USN-3822-1
cert-bund: WID-SEC-2022-0667
cert-bund: CB-K18/0936
cert-bund: CB-K18/0905
cert-bund: CB-K18/0701
cert-bund: CB-K18/0153
cert-bund: CB-K18/0049
cert-bund: CB-K17/2192
cert-bund: CB-K17/2144
cert-bund: CB-K17/2103
cert-bund: CB-K17/2098
cert-bund: CB-K17/2055
cert-bund: CB-K17/1286
cert-bund: CB-K17/0866
cert-bund: CB-K17/0812
cert-bund: CB-K17/0552
cert-bund: CB-K17/0401
cert-bund: CB-K17/0317
cert-bund: CB-K16/1981
dfn-cert: DFN-CERT-2019-2615
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-0245
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2019-0020
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2458
dfn-cert: DFN-CERT-2018-2359
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-2346
dfn-cert: DFN-CERT-2018-2344
dfn-cert: DFN-CERT-2018-2294
dfn-cert: DFN-CERT-2018-2279
dfn-cert: DFN-CERT-2018-2262
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2149
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2067
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-2060
dfn-cert: DFN-CERT-2018-2050
dfn-cert: DFN-CERT-2018-2039
dfn-cert: DFN-CERT-2018-1997
dfn-cert: DFN-CERT-2018-1990
dfn-cert: DFN-CERT-2018-1967
dfn-cert: DFN-CERT-2018-1966
dfn-cert: DFN-CERT-2018-1962
dfn-cert: DFN-CERT-2018-1954
dfn-cert: DFN-CERT-2018-1940
dfn-cert: DFN-CERT-2018-1905
dfn-cert: DFN-CERT-2018-1870
dfn-cert: DFN-CERT-2018-1856
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1748
dfn-cert: DFN-CERT-2018-1720
dfn-cert: DFN-CERT-2018-1179
dfn-cert: DFN-CERT-2018-1067
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2017-2291
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2196
dfn-cert: DFN-CERT-2017-2192
dfn-cert: DFN-CERT-2017-2142
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0322
dfn-cert: DFN-CERT-2016-2093
```

High (CVSS: 8.2)
NVT: Ubuntu: Security Advisory (USN-3968-2)

Summary
The remote host is missing an update for the ’sudo’ package(s) announced via the USN-3968-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm1
```

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

Affected Software/OS
’sudo’ package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-3968-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Sudo did not properly parse the contents of /proc/[pid]/stat when attempting to determine its controlling tty. A local attacker in some configurations could possibly use this to overwrite any file on the filesystem, bypassing intended permissions. (CVE-2017-1000368)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3968-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3968.2
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-3968-2
cve: CVE-2017-1000368
advisory_id: USN-3968-2
cert-bund: CB-K17/0909
dfn-cert: DFN-CERT-2019-0903
dfn-cert: DFN-CERT-2017-0940
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5068-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'libgd2' package(s) announced via the USN-5068-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libgd3
Installed version:    libgd3-2.1.0-3ubuntu0.11
Fixed version:      >=libgd3-2.1.0-3ubuntu0.11+esm2
```

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.

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: `2022-09-13T14:14:11Z`

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-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-4386-1)

Summary
The remote host is missing an update for the 'libjpeg-turbo' package(s) announced via the USN-4386-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjpeg-turbo8
Installed version:    libjpeg-turbo8-1.3.0-0ubuntu2.1
Fixed version:      >=libjpeg-turbo8-1.3.0-0ubuntu2.1+esm1
```

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

Affected Software/OS
'libjpeg-turbo' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
It was discovered that libjpeg-turbo incorrectly handled certain PPM files. An attacker could possibly use this issue to access sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4386-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4386.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4386-1
cve: CVE-2020-13790
advisory_id: USN-4386-1
dfn-cert: DFN-CERT-2020-1682
dfn-cert: DFN-CERT-2020-1239
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-3933-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3933-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
```

. . . continues on next page . . .

... continued from previous page ...

```
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.168.179
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that an information leak vulnerability existed in the Bluetooth implementation of the Linux kernel. An attacker within Bluetooth range could possibly expose sensitive information (kernel memory). (CVE-2017-1000410)
It was discovered that the USB serial device driver in the Linux kernel did not properly validate baud rate settings when debugging is enabled. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-18360)
Mathias Payer and Hui Peng discovered a use-after-free vulnerability in the Advanced Linux Sound Architecture (ALSA) subsystem. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2018-19824)
Shlomi Oberman, Yuli Shapiro, and Ran Menscher discovered an information leak in the Bluetooth implementation of the Linux kernel. An attacker within Bluetooth range could use this to expose sensitive information (kernel memory). (CVE-2019-3459, CVE-2019-3460)
Jann Horn discovered that the KVM implementation in the Linux kernel contained a use-after-free vulnerability. An attacker in a guest VM with access to /dev/kvm could use this to cause a denial of service (guest VM crash). (CVE-2019-6974)
Felix Wilhelm discovered that an information leak vulnerability existed in the KVM subsystem of the Linux kernel, when nested virtualization is used. A local attacker could use this to expose sensitive information (host system memory to a guest VM). (CVE-2019-7222)
Jann Horn discovered that the mmap implementation in the Linux kernel did not properly check for the mmap minimum address in some situations. A local attacker could use this to assist exploiting a kernel NULL pointer dereference vulnerability. (CVE-2019-9213)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3933-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3933.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3933-1
cve: CVE-2017-1000410
cve: CVE-2017-18360
cve: CVE-2018-19824
cve: CVE-2019-3459
cve: CVE-2019-3460
```

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2019-6974
cve: CVE-2019-7222
cve: CVE-2019-9213
advisory_id: USN-3933-1
cert-bund: WID-SEC-2022-1300
cert-bund: CB-K20/1030
cert-bund: CB-K19/0881
cert-bund: CB-K19/0192
cert-bund: CB-K19/0151
cert-bund: CB-K19/0146
cert-bund: CB-K19/0041
cert-bund: CB-K18/1139
cert-bund: CB-K18/0165
cert-bund: CB-K18/0051
cert-bund: CB-K17/2223
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2020-2186
dfn-cert: DFN-CERT-2020-0481
dfn-cert: DFN-CERT-2020-0081
dfn-cert: DFN-CERT-2019-2514
dfn-cert: DFN-CERT-2019-2313
dfn-cert: DFN-CERT-2019-2249
dfn-cert: DFN-CERT-2019-2095
dfn-cert: DFN-CERT-2019-1970
dfn-cert: DFN-CERT-2019-1918
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1483
dfn-cert: DFN-CERT-2019-1222
dfn-cert: DFN-CERT-2019-1132
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1017
dfn-cert: DFN-CERT-2019-0996
dfn-cert: DFN-CERT-2019-0915
dfn-cert: DFN-CERT-2019-0894
dfn-cert: DFN-CERT-2019-0821
dfn-cert: DFN-CERT-2019-0759
dfn-cert: DFN-CERT-2019-0758
dfn-cert: DFN-CERT-2019-0701
dfn-cert: DFN-CERT-2019-0677
dfn-cert: DFN-CERT-2019-0675
dfn-cert: DFN-CERT-2019-0673
dfn-cert: DFN-CERT-2019-0672
dfn-cert: DFN-CERT-2019-0658
dfn-cert: DFN-CERT-2019-0637
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0613
dfn-cert: DFN-CERT-2019-0562
dfn-cert: DFN-CERT-2019-0546
dfn-cert: DFN-CERT-2019-0453
dfn-cert: DFN-CERT-2019-0442
dfn-cert: DFN-CERT-2019-0399
dfn-cert: DFN-CERT-2019-0391
dfn-cert: DFN-CERT-2019-0361
dfn-cert: DFN-CERT-2019-0355
dfn-cert: DFN-CERT-2019-0324
dfn-cert: DFN-CERT-2019-0251
dfn-cert: DFN-CERT-2019-0245
dfn-cert: DFN-CERT-2019-0239
dfn-cert: DFN-CERT-2019-0204
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0133
dfn-cert: DFN-CERT-2019-0113
dfn-cert: DFN-CERT-2019-0101
dfn-cert: DFN-CERT-2019-0095
dfn-cert: DFN-CERT-2018-2512
dfn-cert: DFN-CERT-2018-2493
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1170
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0889
dfn-cert: DFN-CERT-2018-0737
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2017-2319
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2293
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-4713-2)

Summary
The remote host is missing an update for the 'linux, linux-gke-5.0, linux-gke-5.3, linux-hwe, linux-raspi2-5.3' package(s) announced via the USN-4713-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.184.193
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'linux, linux-gke-5.0, linux-gke-5.3, linux-hwe, linux-raspi2-5.3' package(s) on Ubuntu 14.04, Ubuntu 18.04.

Vulnerability Insight
It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4713-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4713.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4713-2
cve: CVE-2020-28374
advisory_id: USN-4713-2
cert-bund: WID-SEC-2022-2085
cert-bund: WID-SEC-2022-1308
cert-bund: CB-K21/1268
cert-bund: CB-K21/0025
dfn-cert: DFN-CERT-2021-1563
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1292
dfn-cert: DFN-CERT-2021-1190
dfn-cert: DFN-CERT-2021-1177
dfn-cert: DFN-CERT-2021-1139
dfn-cert: DFN-CERT-2021-1133
dfn-cert: DFN-CERT-2021-1013
dfn-cert: DFN-CERT-2021-0888
dfn-cert: DFN-CERT-2021-0887
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0698
dfn-cert: DFN-CERT-2021-0679
dfn-cert: DFN-CERT-2021-0579
dfn-cert: DFN-CERT-2021-0561
dfn-cert: DFN-CERT-2021-0560
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-0509
dfn-cert: DFN-CERT-2021-0505
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0327
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0313
dfn-cert: DFN-CERT-2021-0282
dfn-cert: DFN-CERT-2021-0280
dfn-cert: DFN-CERT-2021-0277
dfn-cert: DFN-CERT-2021-0261
dfn-cert: DFN-CERT-2021-0247
dfn-cert: DFN-CERT-2021-0221
dfn-cert: DFN-CERT-2021-0192
dfn-cert: DFN-CERT-2021-0191
dfn-cert: DFN-CERT-2021-0116
dfn-cert: DFN-CERT-2021-0105
dfn-cert: DFN-CERT-2021-0100
dfn-cert: DFN-CERT-2021-0099
dfn-cert: DFN-CERT-2021-0082
dfn-cert: DFN-CERT-2021-0081
dfn-cert: DFN-CERT-2021-0080
dfn-cert: DFN-CERT-2021-0073
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-6112-1)

Summary
The remote host is missing an update for the 'perl' package(s) announced via the USN-6112-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   perl
Installed version:    perl-5.18.2-2ubuntu1.7
Fixed version:      >=perl-5.18.2-2ubuntu1.7+esm5
```

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.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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-6112-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6112.1
Version used: `2023-05-30T04:09:22Z`

References

```
url: https://ubuntu.com/security/notices/USN-6112-1
cve: CVE-2023-31484
advisory_id: USN-6112-1
cert-bund: WID-SEC-2023-1608
dfn-cert: DFN-CERT-2023-1225
```

High (CVSS: 8.1)
NVT: Ubuntu: Security Advisory (USN-5638-4)

Summary

The remote host is missing an update for the 'expat' package(s) announced via the USN-5638-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.1.0-4ubuntu1.4
Fixed version:      >=libexpat1-2.1.0-4ubuntu1.4+esm7
```

Solution:

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

Affected Software/OS

'expat' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-5638-1 fixed several vulnerabilities in Expat. This update provides the corresponding update for Ubuntu 14.04 ESM.
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

. . . 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-5638-4)
OID:1.3.6.1.4.1.25623.1.1.12.2023.5638.4
Version used: 2023-03-02T04:10:54Z

References

url: https://ubuntu.com/security/notices/USN-5638-4
cve: CVE-2022-40674
cve: CVE-2022-43680
advisory_id: USN-5638-4
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-2023-1590
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: 8.0)
NVT: Ubuntu: Security Advisory (USN-3422-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3422-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.132.141
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that a buffer overflow existed in the Bluetooth stack of the Linux kernel when handling L2CAP configuration responses. A physically proximate attacker could use this to cause a denial of service (system crash). (CVE-2017-1000251)
It was discovered that the asynchronous I/O (aio) subsystem of the Linux kernel did not properly set permissions on aio memory mappings in some situations. An attacker could use this to more easily exploit other vulnerabilities. (CVE-2016-10044)
Baozeng Ding and Andrey Konovalov discovered a race condition in the L2TPv3 IP Encapsulation 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-2016-10200)
Andreas Gruenbacher and Jan Kara discovered that the filesystem implementation in the Linux kernel did not clear the setgid bit during a setxattr call. A local attacker could use this to possibly elevate group privileges. (CVE-2016-7097)
Sergej Schumilo, Ralf Spenneberg, and Hendrik Schwartke discovered that the key management subsystem in the Linux kernel did not properly allocate memory in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2016-8650)
Vlad Tsyrklevich discovered an integer overflow vulnerability in the VFIO PCI driver for the Linux kernel. A local attacker with access to a vfio PCI device file could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2016-9083, CVE-2016-9084)
It was discovered that an information leak existed in __get_user_asm_ex() in the Linux kernel. A local attacker could use this to expose sensitive information. (CVE-2016-9178)
CAI Qian discovered that the sysctl implementation in the Linux kernel did not properly perform reference counting in some situations. An unprivileged attacker could use this to cause a denial of service (system hang). (CVE-2016-9191)
It was discovered that the keyring implementation in the Linux kernel in some situations did not prevent special internal keyrings from being joined by userspace keyrings. A privileged local attacker could use this to bypass module verification. (CVE-2016-9604)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that an integer overflow existed in the trace subsystem of the Linux kernel. A local privileged attacker could use this to cause a denial of service (system crash). (CVE-2016-9754)
Andrey Konovalov discovered that the IPv4 implementation in the Linux kernel did not properly handle invalid IP options in some situations. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2017-5970)
Dmitry Vyukov discovered that the Linux kernel did not properly handle TCP packets with the URG flag. A remote attacker could use this to cause a denial of service. (CVE-2017-6214)
It was discovered that a race condition existed in the AF_PACKET ... [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-3422-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3422.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3422-1
cve: CVE-2016-10044
cve: CVE-2016-10200
cve: CVE-2016-7097
cve: CVE-2016-8650
cve: CVE-2016-9083
cve: CVE-2016-9084
cve: CVE-2016-9178
cve: CVE-2016-9191
cve: CVE-2016-9604
cve: CVE-2016-9754
cve: CVE-2017-1000251
cve: CVE-2017-5970
cve: CVE-2017-6214
cve: CVE-2017-6346
cve: CVE-2017-6951
cve: CVE-2017-7187
cve: CVE-2017-7472
cve: CVE-2017-7541
advisory_id: USN-3422-1
cert-bund: WID-SEC-2022-1612
cert-bund: WID-SEC-2022-1345
cert-bund: CB-K18/0184
cert-bund: CB-K18/0173
cert-bund: CB-K18/0153
cert-bund: CB-K18/0049
cert-bund: CB-K18/0017
cert-bund: CB-K17/2169
cert-bund: CB-K17/2141
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/2125
cert-bund: CB-K17/2124
cert-bund: CB-K17/2008
cert-bund: CB-K17/1940
cert-bund: CB-K17/1908
cert-bund: CB-K17/1901
cert-bund: CB-K17/1892
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1867
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1830
cert-bund: CB-K17/1801
cert-bund: CB-K17/1781
cert-bund: CB-K17/1776
cert-bund: CB-K17/1769
cert-bund: CB-K17/1696
cert-bund: CB-K17/1678
cert-bund: CB-K17/1649
cert-bund: CB-K17/1607
cert-bund: CB-K17/1602
cert-bund: CB-K17/1584
cert-bund: CB-K17/1578
cert-bund: CB-K17/1568
cert-bund: CB-K17/1567
cert-bund: CB-K17/1545
cert-bund: CB-K17/1530
cert-bund: CB-K17/1520
cert-bund: CB-K17/1505
cert-bund: CB-K17/1491
cert-bund: CB-K17/1484
cert-bund: CB-K17/1452
cert-bund: CB-K17/1449
cert-bund: CB-K17/1419
cert-bund: CB-K17/1408
cert-bund: CB-K17/1404
cert-bund: CB-K17/1346
cert-bund: CB-K17/1345
cert-bund: CB-K17/1325
cert-bund: CB-K17/1286
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1236
cert-bund: CB-K17/1226
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1085
cert-bund: CB-K17/1083
cert-bund: CB-K17/0979
cert-bund: CB-K17/0941
cert-bund: CB-K17/0910
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0836
cert-bund: CB-K17/0834
cert-bund: CB-K17/0826
cert-bund: CB-K17/0825
cert-bund: CB-K17/0812
cert-bund: CB-K17/0773
cert-bund: CB-K17/0764
cert-bund: CB-K17/0746
cert-bund: CB-K17/0719
cert-bund: CB-K17/0716
cert-bund: CB-K17/0697
cert-bund: CB-K17/0690
cert-bund: CB-K17/0648
cert-bund: CB-K17/0628
cert-bund: CB-K17/0611
cert-bund: CB-K17/0579
cert-bund: CB-K17/0552
cert-bund: CB-K17/0549
cert-bund: CB-K17/0546
cert-bund: CB-K17/0484
cert-bund: CB-K17/0401
cert-bund: CB-K17/0394
cert-bund: CB-K17/0391
cert-bund: CB-K17/0370
cert-bund: CB-K17/0354
cert-bund: CB-K17/0326
cert-bund: CB-K17/0325
cert-bund: CB-K17/0317
cert-bund: CB-K17/0305
cert-bund: CB-K17/0297
cert-bund: CB-K17/0293
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0220
cert-bund: CB-K17/0216
cert-bund: CB-K17/0212
cert-bund: CB-K17/0211
cert-bund: CB-K17/0168
cert-bund: CB-K17/0157
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K17/0088
cert-bund: CB-K17/0013
cert-bund: CB-K17/0011
cert-bund: CB-K17/0001
cert-bund: CB-K16/1999
cert-bund: CB-K16/1913
cert-bund: CB-K16/1901
cert-bund: CB-K16/1900
cert-bund: CB-K16/1878
cert-bund: CB-K16/1869
cert-bund: CB-K16/1863
cert-bund: CB-K16/1859
cert-bund: CB-K16/1843
cert-bund: CB-K16/1763
cert-bund: CB-K16/1690
dfn-cert: DFN-CERT-2022-2194
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0184
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2224
dfn-cert: DFN-CERT-2017-2099
dfn-cert: DFN-CERT-2017-2023
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1986
dfn-cert: DFN-CERT-2017-1972
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1913
dfn-cert: DFN-CERT-2017-1884
dfn-cert: DFN-CERT-2017-1862
dfn-cert: DFN-CERT-2017-1852
dfn-cert: DFN-CERT-2017-1850
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1759
dfn-cert: DFN-CERT-2017-1726
dfn-cert: DFN-CERT-2017-1678
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1669
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1646
dfn-cert: DFN-CERT-2017-1637
dfn-cert: DFN-CERT-2017-1632
dfn-cert: DFN-CERT-2017-1616
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1570
dfn-cert: DFN-CERT-2017-1556
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1518
dfn-cert: DFN-CERT-2017-1513
dfn-cert: DFN-CERT-2017-1477
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1467
dfn-cert: DFN-CERT-2017-1405
dfn-cert: DFN-CERT-2017-1404
dfn-cert: DFN-CERT-2017-1376
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1278
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-1120
dfn-cert: DFN-CERT-2017-1119
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0943
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0863
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0850
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0799
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0771
dfn-cert: DFN-CERT-2017-0743
dfn-cert: DFN-CERT-2017-0737
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0713
dfn-cert: DFN-CERT-2017-0666
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0649
dfn-cert: DFN-CERT-2017-0622
dfn-cert: DFN-CERT-2017-0604
dfn-cert: DFN-CERT-2017-0569
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0496
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0402
dfn-cert: DFN-CERT-2017-0394
dfn-cert: DFN-CERT-2017-0377
dfn-cert: DFN-CERT-2017-0359
dfn-cert: DFN-CERT-2017-0331
dfn-cert: DFN-CERT-2017-0327
dfn-cert: DFN-CERT-2017-0322
dfn-cert: DFN-CERT-2017-0311
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0297
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0225
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0217
dfn-cert: DFN-CERT-2017-0216
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0158
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2017-0011
dfn-cert: DFN-CERT-2017-0010
dfn-cert: DFN-CERT-2017-0001
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2013
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-1984
dfn-cert: DFN-CERT-2016-1975
dfn-cert: DFN-CERT-2016-1967
dfn-cert: DFN-CERT-2016-1959
dfn-cert: DFN-CERT-2016-1948
dfn-cert: DFN-CERT-2016-1867
dfn-cert: DFN-CERT-2016-1784
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4889-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux, linux-lts-xenial' package(s) announced via the USN-4889-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.185.194
```

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

Affected Software/OS
'linux, linux-lts-xenial' package(s) on Ubuntu 14.04.

Vulnerability Insight
Adam Nichols discovered that heap overflows existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2021-27365)
Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did not properly restrict access to iSCSI transport handles. A local attacker could use this to cause a denial of service or expose sensitive information (kernel pointer addresses). (CVE-2021-27363)
Adam Nichols discovered that an out-of-bounds read existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information (kernel memory). (CVE-2021-27364)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4889-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4889.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4889-1
cve: CVE-2021-27363
cve: CVE-2021-27364
cve: CVE-2021-27365
advisory_id: USN-4889-1
cert-bund: WID-SEC-2022-2077
cert-bund: WID-SEC-2022-1308
cert-bund: CB-K21/1268
cert-bund: CB-K21/0240
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1295
dfn-cert: DFN-CERT-2021-1052
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1026
dfn-cert: DFN-CERT-2021-1022
dfn-cert: DFN-CERT-2021-1013
dfn-cert: DFN-CERT-2021-0888
dfn-cert: DFN-CERT-2021-0887
dfn-cert: DFN-CERT-2021-0825
dfn-cert: DFN-CERT-2021-0824
dfn-cert: DFN-CERT-2021-0823
dfn-cert: DFN-CERT-2021-0822
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-2021-0740
dfn-cert: DFN-CERT-2021-0737
dfn-cert: DFN-CERT-2021-0731
dfn-cert: DFN-CERT-2021-0713
dfn-cert: DFN-CERT-2021-0699
dfn-cert: DFN-CERT-2021-0698
dfn-cert: DFN-CERT-2021-0697
dfn-cert: DFN-CERT-2021-0688
dfn-cert: DFN-CERT-2021-0679
dfn-cert: DFN-CERT-2021-0658
dfn-cert: DFN-CERT-2021-0655
dfn-cert: DFN-CERT-2021-0614
dfn-cert: DFN-CERT-2021-0564
dfn-cert: DFN-CERT-2021-0505
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5014-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-gcp, linux-gke-5.3, linux-hwe, linux-kvm, linux-lts-xenial, linux-oracle, linux-raspi, linux-raspi2-5.3' package(s) announced via the USN-5014-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.186.195
```

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-azure, linux-gcp, linux-gke-5.3, linux-hwe, linux-kvm, linux-lts-xenial, linux-oracle, linux-raspi, linux-raspi2-5.3' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 21.04.

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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5014-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5014.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5014-1
cve: CVE-2021-33909
advisory_id: USN-5014-1
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-0965
cert-bund: WID-SEC-2022-0624
cert-bund: CB-K21/1268
cert-bund: CB-K21/1251
cert-bund: CB-K21/0775
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-2021-1920
dfn-cert: DFN-CERT-2021-1802
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-2021-1653
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5039-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-kvm, linux-lts-xenial' package(s) announced via the USN-5039-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.187.196
```

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

Affected Software/OS
'linux, linux-aws, linux-kvm, linux-lts-xenial' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
Andy Nguyen discovered that the netfilter subsystem in the Linux kernel contained an out-of-bounds write in its setsockopt() implementation. 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.
Details: `Ubuntu: Security Advisory (USN-5039-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5039.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-5039-1
cve: CVE-2021-22555
advisory_id: USN-5039-1
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-0609
cert-bund: CB-K21/1268
cert-bund: CB-K21/0727
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0026
dfn-cert: DFN-CERT-2021-2157
dfn-cert: DFN-CERT-2021-2156
dfn-cert: DFN-CERT-2021-2071
dfn-cert: DFN-CERT-2021-1924
dfn-cert: DFN-CERT-2021-1920
dfn-cert: DFN-CERT-2021-1905
dfn-cert: DFN-CERT-2021-1852
dfn-cert: DFN-CERT-2021-1846
dfn-cert: DFN-CERT-2021-1845
dfn-cert: DFN-CERT-2021-1842
dfn-cert: DFN-CERT-2021-1837
dfn-cert: DFN-CERT-2021-1836
dfn-cert: DFN-CERT-2021-1783
dfn-cert: DFN-CERT-2021-1761
dfn-cert: DFN-CERT-2021-1742
dfn-cert: DFN-CERT-2021-1703
dfn-cert: DFN-CERT-2021-1696
dfn-cert: DFN-CERT-2021-1653
dfn-cert: DFN-CERT-2021-1634
dfn-cert: DFN-CERT-2021-1617
dfn-cert: DFN-CERT-2021-1574
dfn-cert: DFN-CERT-2021-1571
dfn-cert: DFN-CERT-2021-1546
dfn-cert: DFN-CERT-2021-1544
dfn-cert: DFN-CERT-2021-1535
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5130-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-5130-1 advisory.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.188.197
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

Jann Horn discovered a race condition in the tty subsystem of the Linux kernel in the locking for the TIOCSPGRP ioctl(), 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-2020-29661) Jann Horn discovered that the tty subsystem of the Linux kernel did not use consistent locking in some situations, leading to a read-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). (CVE-2020-29660)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-5130-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2021.5130.1

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5130-1
cve: CVE-2020-29660
cve: CVE-2020-29661
advisory_id: USN-5130-1
cert-bund: WID-SEC-2022-1308
cert-bund: WID-SEC-2022-0623
cert-bund: CB-K21/1268
cert-bund: CB-K21/1032
cert-bund: CB-K21/0472
cert-bund: CB-K20/1225
dfn-cert: DFN-CERT-2021-2399
dfn-cert: DFN-CERT-2021-2390
dfn-cert: DFN-CERT-2021-2347
dfn-cert: DFN-CERT-2021-2058
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1178
dfn-cert: DFN-CERT-2021-0925
dfn-cert: DFN-CERT-2021-0823
dfn-cert: DFN-CERT-2021-0715
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-0586
dfn-cert: DFN-CERT-2021-0574
dfn-cert: DFN-CERT-2021-0561
dfn-cert: DFN-CERT-2021-0560
dfn-cert: DFN-CERT-2021-0505
dfn-cert: DFN-CERT-2021-0497
dfn-cert: DFN-CERT-2021-0496
dfn-cert: DFN-CERT-2021-0468
dfn-cert: DFN-CERT-2021-0467
dfn-cert: DFN-CERT-2021-0426
dfn-cert: DFN-CERT-2021-0425
dfn-cert: DFN-CERT-2021-0424
dfn-cert: DFN-CERT-2021-0423
dfn-cert: DFN-CERT-2021-0422
dfn-cert: DFN-CERT-2021-0364
dfn-cert: DFN-CERT-2021-0356
dfn-cert: DFN-CERT-2021-0342
dfn-cert: DFN-CERT-2021-0330
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2021-0326
dfn-cert: DFN-CERT-2021-0309
dfn-cert: DFN-CERT-2021-0277
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0261
dfn-cert: DFN-CERT-2021-0247
dfn-cert: DFN-CERT-2021-0221
dfn-cert: DFN-CERT-2021-0116
dfn-cert: DFN-CERT-2021-0105
dfn-cert: DFN-CERT-2021-0100
dfn-cert: DFN-CERT-2021-0099
dfn-cert: DFN-CERT-2021-0084
dfn-cert: DFN-CERT-2021-0079
dfn-cert: DFN-CERT-2021-0077
dfn-cert: DFN-CERT-2021-0076
dfn-cert: DFN-CERT-2021-0075
dfn-cert: DFN-CERT-2020-2715
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5760-2)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-5760-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.1+dfsg1-3ubuntu4.13
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libxml2-2.9.1+dfsg1-3ubuntu4.13+esm4
```

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5760-1 fixed vulnerabilities in libxml2. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5760-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5760.2
Version used: `2022-12-06T04:10:22Z`

References

```
url: https://ubuntu.com/security/notices/USN-5760-2
cve: CVE-2022-40303
cve: CVE-2022-40304
advisory_id: USN-5760-2
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-1350
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
dfn-cert: DFN-CERT-2023-1590
dfn-cert: DFN-CERT-2023-1022
dfn-cert: DFN-CERT-2023-0881
dfn-cert: DFN-CERT-2023-0372
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5452-1)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5452-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ntfs-3g
Installed version:    ntfs-3g-1:2013.1.13AR.1-2ubuntu2
Fixed version:      >=ntfs-3g-1:2013.1.13AR.1-2ubuntu2+esm2
```

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that NTFS-3G was incorrectly validating NTFS metadata in its ntfsck tool by not performing boundary checks. A local attacker could possibly use this issue to cause a denial of service 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-5452-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5452.1
Version used: `2022-09-21T04:42:37Z`

References

```
url: https://ubuntu.com/security/notices/USN-5452-1
cve: CVE-2021-46790
advisory_id: USN-5452-1
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: WID-SEC-2023-1185
dfn-cert: DFN-CERT-2023-1117
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-5463-2)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5463-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ntfs-3g
Installed version:    ntfs-3g-1:2013.1.13AR.1-2ubuntu2
Fixed version:      >=ntfs-3g-1:2013.1.13AR.1-2ubuntu2+esm3
```

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5463-1 fixed vulnerabilities in NTFS-3G. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5463-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5463.2

... continues on next page ...

. . . continued from previous page . . .

Version used: `2022-09-29T12:44:30Z`

References

```
url: https://ubuntu.com/security/notices/USN-5463-2
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-5463-2
cert-bund: WID-SEC-2023-1185
dfn-cert: DFN-CERT-2023-1117
dfn-cert: DFN-CERT-2023-1048
dfn-cert: DFN-CERT-2022-1409
dfn-cert: DFN-CERT-2022-1218
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4058-2)

Summary

The remote host is missing an update for the 'bash' package(s) announced via the USN-4058-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   bash
Installed version:    bash-4.3-7ubuntu1.7
Fixed version:      >=bash-4.3-7ubuntu1.8+esm1
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'bash' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4058-1 fixed a vulnerability in bash. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.

Original advisory details:

It was discovered that Bash incorrectly handled the restricted shell. An attacker could possibly use this issue to escape restrictions and execute any command.

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-4058-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4058.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4058-2
cve: CVE-2019-9924
advisory_id: USN-4058-2
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K19/0284
dfn-cert: DFN-CERT-2019-0659
dfn-cert: DFN-CERT-2019-0596
```

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.

Vulnerability Detection Result

```
Vulnerable package:   bash
Installed version:    bash-4.3-7ubuntu1.7
Fixed version:      >=bash-4.3-7ubuntu1.8+esm2
```

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.

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: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5380-1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2019-18276
advisory_id: USN-5380-1
cert-bund: WID-SEC-2022-1908
cert-bund: CB-K21/0537
dfn-cert: DFN-CERT-2021-1066
```

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.

Vulnerability Detection Result

```
Vulnerable package:   binutils
Installed version:    binutils-2.24-5ubuntu14.2
Fixed version:      >=binutils-2.24-5ubuntu14.2+esm1
```

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

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)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2023.6101.1
Version used: `2023-05-26T04:09:33Z`

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-2023-0900
cert-bund: WID-SEC-2023-0728
dfn-cert: DFN-CERT-2023-1199
dfn-cert: DFN-CERT-2023-0844
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5711-2)

Summary

The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5711-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ntfs-3g
Installed version:    ntfs-3g-1:2013.1.13AR.1-2ubuntu2
Fixed version:      >=ntfs-3g-1:2013.1.13AR.1-2ubuntu2+esm4
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'ntfs-3g' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

USN-5711-1 fixed a vulnerability in NTFS-3G. This update provides the corresponding update for Ubuntu 14.04 ESM Ubuntu 16.04 ESM.
Original advisory details:
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-5711-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5711.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-11-10T04:23:14Z

References

```
url: https://ubuntu.com/security/notices/USN-5711-2
cve: CVE-2022-40284
advisory_id: USN-5711-2
dfn-cert: DFN-CERT-2022-2457
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4487-2)

Summary

The remote host is missing an update for the 'libx11' package(s) announced via the USN-4487-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libx11-6
Installed version:    libx11-6-2:1.6.2-1ubuntu2.1
Fixed version:      >=libx11-6-2:1.6.2-1ubuntu2.1+esm1
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'libx11' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4487-1 fixed several vulnerabilities in libx11. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM.

Original advisory details:

Todd Carson discovered that libx11 incorrectly handled certain memory operations. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14344)

Jayden Rivers discovered that libx11 incorrectly handled locales. A local attacker could possibly use this issue to escalate privileges. (CVE-2020-14363)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-4487-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2020.4487.2

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4487-2
cve: CVE-2020-14344
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-14363
advisory_id: USN-4487-2
cert-bund: CB-K20/0841
dfn-cert: DFN-CERT-2021-1072
dfn-cert: DFN-CERT-2021-0056
dfn-cert: DFN-CERT-2020-2588
dfn-cert: DFN-CERT-2020-2439
dfn-cert: DFN-CERT-2020-1860
dfn-cert: DFN-CERT-2020-1856
dfn-cert: DFN-CERT-2020-1696
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5995-1)

Summary
The remote host is missing an update for the 'vim' package(s) announced via the USN-5995-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:7.4.052-1ubuntu3.1
Fixed version:      >=vim-tiny-2:7.4.052-1ubuntu3.1+esm8
```

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)

. . . 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 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)

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: `2023-04-05T07:23:17Z`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2023-1424
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-2022-1195
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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-4071-2)

Summary
The remote host is missing an update for the 'patch' package(s) announced via the USN-4071-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   patch
Installed version:    patch-2.7.1-4ubuntu2.4
Fixed version:      >=patch-2.7.1-4ubuntu2.4+esm1
```

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

Affected Software/OS
'patch' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4071-1 fixed several vulnerabilities in Patch. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that Patch incorrectly handled certain files. An attacker could possibly use this issue to access sensitive information. (CVE-2019-13636)
It was discovered that Patch incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-13638)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4071-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4071.2
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4071-2
cve: CVE-2019-13636
cve: CVE-2019-13638
advisory_id: USN-4071-2
cert-bund: WID-SEC-2022-0043
cert-bund: CB-K20/1049
cert-bund: CB-K19/0667
dfn-cert: DFN-CERT-2022-1252
dfn-cert: DFN-CERT-2019-1959
dfn-cert: DFN-CERT-2019-1532
dfn-cert: DFN-CERT-2019-1527
dfn-cert: DFN-CERT-2019-1495
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3993-2)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-3993-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm2
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm2
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'curl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-3993-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that curl incorrectly handled memory when receiving data from a TFTP 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-2019-5436)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3993-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3993.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3993-2
cve: CVE-2019-5436
advisory_id: USN-3993-2
cert-bund: WID-SEC-2023-1639
cert-bund: CB-K20/1049
cert-bund: CB-K19/0915
cert-bund: CB-K19/0909
cert-bund: CB-K19/0444
dfn-cert: DFN-CERT-2020-0670
dfn-cert: DFN-CERT-2020-0555
dfn-cert: DFN-CERT-2020-0390
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-1051
```

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.

Vulnerability Detection Result

```
Vulnerable package:   perl
Installed version:    perl-5.18.2-2ubuntu1.7
Fixed version:      >=perl-5.18.2-2ubuntu1.7+esm4
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2022-10-20T04:36:45Z`

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-4402-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-4402-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm4
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm4
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm4
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'curl' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
Marek Szlagor, Gregory Jefferis and Jeroen Ooms discovered that curl incorrectly handled certain credentials. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-8169)
It was discovered that curl incorrectly handled certain parameters. An attacker could possibly use this issue to overwrite a local file. (CVE-2020-8177)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4402-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4402.1
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4402-1
cve: CVE-2020-8169
cve: CVE-2020-8177
advisory_id: USN-4402-1
cert-bund: WID-SEC-2023-1636
cert-bund: WID-SEC-2023-1350
cert-bund: CB-K20/0684
cert-bund: CB-K20/0619
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2770
dfn-cert: DFN-CERT-2020-2588
dfn-cert: DFN-CERT-2020-2550
dfn-cert: DFN-CERT-2020-1348
dfn-cert: DFN-CERT-2020-1347
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5252-2)

Summary
The remote host is missing an update for the 'policykit-1' package(s) announced via the USN-5252-2 advisory.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   policykit-1
Installed version:    policykit-1-0.105-4ubuntu3.14.04.6
Fixed version:      >=policykit-1-0.105-4ubuntu3.14.04.6+esm1
```

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

Affected Software/OS
'policykit-1' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5252-1 fixed a vulnerability in policykit-1. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5252-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5252.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-5252-2
cve: CVE-2021-4034
advisory_id: USN-5252-2
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-3250-1)

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'linux' package(s) announced via the USN-3250-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.115.125
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

It was discovered that the xfrm framework for transforming packets in the Linux kernel did not properly validate data received from user space. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code with administrative privileges.

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3250-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2017.3250.1

Version used: `2023-02-13T04:10:52Z`

References

```
url: https://ubuntu.com/security/notices/USN-3250-1
cve: CVE-2017-7184
advisory_id: USN-3250-1
cert-bund: CB-K17/1776
cert-bund: CB-K17/1584
cert-bund: CB-K17/1484
cert-bund: CB-K17/1267
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0834
cert-bund: CB-K17/0826
cert-bund: CB-K17/0792
cert-bund: CB-K17/0727
cert-bund: CB-K17/0648
cert-bund: CB-K17/0546
cert-bund: CB-K17/0545
cert-bund: CB-K17/0538
dfn-cert: DFN-CERT-2019-2614
dfn-cert: DFN-CERT-2017-1852
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0820
dfn-cert: DFN-CERT-2017-0742
dfn-cert: DFN-CERT-2017-0666
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0562
dfn-cert: DFN-CERT-2017-0554
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3798-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3798-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.161.171
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Dmitry Vyukov discovered that the key management subsystem in the Linux kernel did not properly restrict adding a key that already exists but is negatively instantiated. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2015-8539)
It was discovered that a use-after-free vulnerability existed in the device driver for XCeive xc2028/xc3028 tuners in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2016-7913)
Pengfei Ding (Ding Peng Fei), Chenfu Bao (Bao Chen Fu), and Lenx Wei (Wei Tao) discovered a race condition in the generic SCSI driver (sg) of the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-0794)

. . . continues on next page . . .

... continued from previous page ...

Eric Biggers discovered that the key management subsystem in the Linux kernel did not properly restrict adding a key that already exists but is uninstantiated. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-15299)
It was discovered that a NULL pointer dereference could be triggered in the OCFS2 file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-18216)
Luo Quan and Wei Yang discovered that a race condition existed in the Advanced Linux Sound Architecture (ALSA) subsystem of the Linux kernel when handling ioctl()s. A local attacker could use this to cause a denial of service (system deadlock). (CVE-2018-1000004)
Fan Long Fei discovered that a race condition existed in the Advanced Linux Sound Architecture (ALSA) subsystem of the Linux kernel that could lead to a use- after-free or an out-of-bounds buffer access. A local attacker with access to /dev/snd/seq could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-7566)
It was discovered that a buffer overflow existed in the NFC Logical Link Control Protocol (llcp) implementation in the Linux kernel. An attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-9518)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3798-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3798.1
Version used: `2022-12-12T04:10:32Z`

References

```
url: https://ubuntu.com/security/notices/USN-3798-1
cve: CVE-2015-8539
cve: CVE-2016-7913
cve: CVE-2017-0794
cve: CVE-2017-15299
cve: CVE-2017-18216
cve: CVE-2018-1000004
cve: CVE-2018-7566
cve: CVE-2018-9518
advisory_id: USN-3798-1
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K18/0898
cert-bund: CB-K18/0635
cert-bund: CB-K18/0560
cert-bund: CB-K18/0550
cert-bund: CB-K18/0367
cert-bund: CB-K18/0347
cert-bund: CB-K18/0250
cert-bund: CB-K18/0173
cert-bund: CB-K18/0160
cert-bund: CB-K17/2129
cert-bund: CB-K17/2008
cert-bund: CB-K17/1998
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K17/1772
cert-bund: CB-K17/1505
cert-bund: CB-K17/1491
cert-bund: CB-K17/0941
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0212
cert-bund: CB-K17/0088
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
cert-bund: CB-K16/1900
cert-bund: CB-K16/1739
cert-bund: CB-K16/1250
cert-bund: CB-K16/1176
cert-bund: CB-K16/0653
cert-bund: CB-K16/0482
cert-bund: CB-K16/0312
cert-bund: CB-K16/0195
cert-bund: CB-K16/0159
cert-bund: CB-K16/0081
dfn-cert: DFN-CERT-2021-2105
dfn-cert: DFN-CERT-2020-2522
dfn-cert: DFN-CERT-2020-2450
dfn-cert: DFN-CERT-2019-1216
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0027
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2018-2525
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2150
dfn-cert: DFN-CERT-2018-2067
dfn-cert: DFN-CERT-2018-1995
dfn-cert: DFN-CERT-2018-1829
dfn-cert: DFN-CERT-2018-1794
dfn-cert: DFN-CERT-2018-1668
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1623
dfn-cert: DFN-CERT-2018-0947
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0932
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0799
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0780
dfn-cert: DFN-CERT-2018-0765
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0184
dfn-cert: DFN-CERT-2018-0178
dfn-cert: DFN-CERT-2017-2223
dfn-cert: DFN-CERT-2017-2099
dfn-cert: DFN-CERT-2017-2092
dfn-cert: DFN-CERT-2017-1847
dfn-cert: DFN-CERT-2017-1570
dfn-cert: DFN-CERT-2017-1556
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2016-1329
dfn-cert: DFN-CERT-2016-1249
dfn-cert: DFN-CERT-2016-0704
dfn-cert: DFN-CERT-2016-0522
dfn-cert: DFN-CERT-2016-0340
dfn-cert: DFN-CERT-2016-0215
dfn-cert: DFN-CERT-2016-0175
dfn-cert: DFN-CERT-2016-0090
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3168-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-3168-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.107.115
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Dmitry Vyukov discovered that the KVM implementation in the Linux kernel did not properly initialize the Code Segment (CS) in certain error cases. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2016-9756)
Andrey Konovalov discovered that signed integer overflows existed in the setsockopt() system call when handling the SO_SNDBUFFORCE and SO_RCVBUFFORCE options. A local attacker with the CAP_NET_ADMIN capability could use this to cause a denial of service (system crash or memory corruption). (CVE-2016-9793)
Baozeng Ding discovered a race condition that could lead to a use-after- free in the Advanced Linux Sound Architecture (ALSA) subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2016-9794)
Baozeng Ding discovered a double free in the netlink_dump() function in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2016-9806)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3168-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3168.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3168-1
cve: CVE-2016-9756
cve: CVE-2016-9793
cve: CVE-2016-9794
cve: CVE-2016-9806
advisory_id: USN-3168-1
cert-bund: CB-K17/1520
cert-bund: CB-K17/1286
cert-bund: CB-K17/0792
cert-bund: CB-K17/0727
cert-bund: CB-K17/0697
cert-bund: CB-K17/0628
cert-bund: CB-K17/0552
cert-bund: CB-K17/0394
cert-bund: CB-K17/0391
cert-bund: CB-K17/0354
cert-bund: CB-K17/0297
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0260
cert-bund: CB-K17/0259
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0168
cert-bund: CB-K17/0122
cert-bund: CB-K17/0088
cert-bund: CB-K17/0063
cert-bund: CB-K17/0047
cert-bund: CB-K17/0004
cert-bund: CB-K16/1954
cert-bund: CB-K16/1928
cert-bund: CB-K16/1913
cert-bund: CB-K16/1900
cert-bund: CB-K16/1874
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0820
dfn-cert: DFN-CERT-2017-0742
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0649
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0402
dfn-cert: DFN-CERT-2017-0394
dfn-cert: DFN-CERT-2017-0359
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0265
dfn-cert: DFN-CERT-2017-0264
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0124
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2017-0063
dfn-cert: DFN-CERT-2017-0050
dfn-cert: DFN-CERT-2017-0003
dfn-cert: DFN-CERT-2016-2070
dfn-cert: DFN-CERT-2016-2034
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-1980
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3149-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3149-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.105.113
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Philip Pettersson discovered a race condition in the af_packet implementation in the Linux kernel. A local unprivileged attacker could use this to cause a denial of service (system crash) or run arbitrary code with administrative privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3149-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2016.3149.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3149-1
cve: CVE-2016-8655
advisory_id: USN-3149-1
cert-bund: CB-K17/0394
cert-bund: CB-K17/0391
cert-bund: CB-K17/0370
cert-bund: CB-K17/0212
cert-bund: CB-K17/0063
cert-bund: CB-K16/1936
cert-bund: CB-K16/1928
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
cert-bund: CB-K16/1900
cert-bund: CB-K16/1890
cert-bund: CB-K16/1877
dfn-cert: DFN-CERT-2017-0402
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0394
dfn-cert: DFN-CERT-2017-0377
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0063
dfn-cert: DFN-CERT-2016-2049
dfn-cert: DFN-CERT-2016-2034
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-2004
dfn-cert: DFN-CERT-2016-1982
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3849-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3849-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.164.174
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that a NULL pointer dereference existed in the keyring subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-2647)
It was discovered that a race condition existed in the raw MIDI driver for the Linux kernel, leading to a double free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-10902)
It was discovered that an integer overrun vulnerability existed in the POSIX timers implementation in the Linux kernel. A local attacker could use this to cause a denial of service. (CVE-2018-12896)
Noam Rathaus discovered that a use-after-free vulnerability existed in the Infiniband implementation in the Linux kernel. An attacker could use this to cause a denial of service (system crash). (CVE-2018-14734)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the YUREX USB device driver for the Linux kernel did not properly restrict user space reads or writes. A physically proximate attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-16276)
Tetsuo Handa discovered a logic error in the TTY subsystem of the Linux kernel. A local attacker with access to pseudo terminal devices could use this to cause a denial of service. (CVE-2018-18386)
Kanda Motohiro discovered that writing extended attributes to an XFS file system in the Linux kernel in certain situations could cause an error condition to occur. A local attacker could use this to cause a denial of service. (CVE-2018-18690)
It was discovered that an integer overflow vulnerability existed in the CDROM driver of the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2018-18710)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3849-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3849.1
Version used: `2023-02-27T04:10:43Z`

References

```
url: https://ubuntu.com/security/notices/USN-3849-1
cve: CVE-2017-2647
cve: CVE-2018-10902
cve: CVE-2018-12896
cve: CVE-2018-14734
cve: CVE-2018-16276
cve: CVE-2018-18386
cve: CVE-2018-18690
cve: CVE-2018-18710
advisory_id: USN-3849-1
cert-bund: CB-K18/1104
cert-bund: CB-K18/1041
cert-bund: CB-K18/0936
cert-bund: CB-K18/0889
cert-bund: CB-K18/0874
cert-bund: CB-K18/0827
cert-bund: CB-K17/1849
cert-bund: CB-K17/1584
cert-bund: CB-K17/1530
cert-bund: CB-K17/1484
cert-bund: CB-K17/1345
cert-bund: CB-K17/1286
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0834
dfn-cert: DFN-CERT-2021-0342
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2092
dfn-cert: DFN-CERT-2020-1857
dfn-cert: DFN-CERT-2019-2514
dfn-cert: DFN-CERT-2019-2246
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1405
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0821
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0607
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0411
dfn-cert: DFN-CERT-2019-0361
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0115
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2018-2604
dfn-cert: DFN-CERT-2018-2603
dfn-cert: DFN-CERT-2018-2602
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2526
dfn-cert: DFN-CERT-2018-2525
dfn-cert: DFN-CERT-2018-2512
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2497
dfn-cert: DFN-CERT-2018-2458
dfn-cert: DFN-CERT-2018-2442
dfn-cert: DFN-CERT-2018-2436
dfn-cert: DFN-CERT-2018-2398
dfn-cert: DFN-CERT-2018-2366
dfn-cert: DFN-CERT-2018-2359
dfn-cert: DFN-CERT-2018-2355
dfn-cert: DFN-CERT-2018-2351
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-2304
dfn-cert: DFN-CERT-2018-2294
dfn-cert: DFN-CERT-2018-2280
dfn-cert: DFN-CERT-2018-2279
dfn-cert: DFN-CERT-2018-2252
dfn-cert: DFN-CERT-2018-2233
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2167
dfn-cert: DFN-CERT-2018-2149
dfn-cert: DFN-CERT-2018-2129
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-2060
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-2050
dfn-cert: DFN-CERT-2018-2039
dfn-cert: DFN-CERT-2018-2023
dfn-cert: DFN-CERT-2018-1997
dfn-cert: DFN-CERT-2018-1995
dfn-cert: DFN-CERT-2018-1990
dfn-cert: DFN-CERT-2018-1978
dfn-cert: DFN-CERT-2018-1967
dfn-cert: DFN-CERT-2018-1966
dfn-cert: DFN-CERT-2018-1962
dfn-cert: DFN-CERT-2018-1941
dfn-cert: DFN-CERT-2018-1940
dfn-cert: DFN-CERT-2018-1911
dfn-cert: DFN-CERT-2018-1905
dfn-cert: DFN-CERT-2018-1870
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1748
dfn-cert: DFN-CERT-2018-1677
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1661
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1654
dfn-cert: DFN-CERT-2018-1631
dfn-cert: DFN-CERT-2018-1535
dfn-cert: DFN-CERT-2018-1348
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1404
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3145-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3145-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.103.111
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Marco Grassi discovered that the driver for Areca RAID Controllers in the Linux kernel did not properly validate control messages. A local attacker could use this to cause a denial of service (system crash) or possibly gain privileges. (CVE-2016-7425)
Daxing Guo discovered a stack-based buffer overflow in the Broadcom IEEE802.11n FullMAC driver in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly gain privileges. (CVE-2016-8658)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3145-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2016.3145.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3145-1
cve: CVE-2016-7425
cve: CVE-2016-8658
advisory_id: USN-3145-1
cert-bund: CB-K17/0838
cert-bund: CB-K17/0552
cert-bund: CB-K17/0297
cert-bund: CB-K17/0277
cert-bund: CB-K17/0168
cert-bund: CB-K17/0088
cert-bund: CB-K17/0001
cert-bund: CB-K16/1999
cert-bund: CB-K16/1925
cert-bund: CB-K16/1878
cert-bund: CB-K16/1869
cert-bund: CB-K16/1859
cert-bund: CB-K16/1843
cert-bund: CB-K16/1657
cert-bund: CB-K16/1641
cert-bund: CB-K16/1627
cert-bund: CB-K16/1455
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0564
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2017-0001
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2033
dfn-cert: DFN-CERT-2016-1984
dfn-cert: DFN-CERT-2016-1975
dfn-cert: DFN-CERT-2016-1967
dfn-cert: DFN-CERT-2016-1948
dfn-cert: DFN-CERT-2016-1754
dfn-cert: DFN-CERT-2016-1741
dfn-cert: DFN-CERT-2016-1731
dfn-cert: DFN-CERT-2016-1546
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3880-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3880-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.165.175
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that the CIFS client implementation in the Linux kernel did not properly handle setup negotiation during session recovery, leading to a NULL pointer exception. An attacker could use this to create a malicious CIFS server that caused a denial of service (client system crash). (CVE-2018-1066)
Jann Horn discovered that the procfs file system implementation in the Linux kernel did not properly restrict the ability to inspect the kernel stack of an arbitrary task. A local attacker could use this to expose sensitive information. (CVE-2018-17972)

. . . continues on next page . . .

. . . continued from previous page . . .

Jann Horn discovered that the mremap() system call in the Linux kernel did not properly flush the TLB when completing, potentially leaving access to a physical page after it has been released to the page allocator. A local attacker could use this to cause a denial of service (system crash), expose sensitive information, or possibly execute arbitrary code. (CVE-2018-18281)
It was discovered that the socket implementation in the Linux kernel contained a type confusion error that could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-9568)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3880-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3880.1
Version used: `2023-02-27T04:10:43Z`

References

```
url: https://ubuntu.com/security/notices/USN-3880-1
cve: CVE-2018-1066
cve: CVE-2018-17972
cve: CVE-2018-18281
cve: CVE-2018-9568
advisory_id: USN-3880-1
cert-bund: WID-SEC-2022-0627
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K19/0014
cert-bund: CB-K18/1193
cert-bund: CB-K18/1140
cert-bund: CB-K18/0962
cert-bund: CB-K18/0635
cert-bund: CB-K18/0550
dfn-cert: DFN-CERT-2020-1179
dfn-cert: DFN-CERT-2020-1178
dfn-cert: DFN-CERT-2020-0143
dfn-cert: DFN-CERT-2020-0081
dfn-cert: DFN-CERT-2020-0070
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2020-0023
dfn-cert: DFN-CERT-2019-2614
dfn-cert: DFN-CERT-2019-2613
dfn-cert: DFN-CERT-2019-2551
dfn-cert: DFN-CERT-2019-2514
dfn-cert: DFN-CERT-2019-1909
dfn-cert: DFN-CERT-2019-1907
dfn-cert: DFN-CERT-2019-1701
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1234
dfn-cert: DFN-CERT-2019-1225
dfn-cert: DFN-CERT-2019-1032
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0821
dfn-cert: DFN-CERT-2019-0649
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0546
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0530
dfn-cert: DFN-CERT-2019-0495
dfn-cert: DFN-CERT-2019-0453
dfn-cert: DFN-CERT-2019-0361
dfn-cert: DFN-CERT-2019-0316
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0259
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0251
dfn-cert: DFN-CERT-2019-0240
dfn-cert: DFN-CERT-2019-0211
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2019-0185
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0133
dfn-cert: DFN-CERT-2019-0115
dfn-cert: DFN-CERT-2019-0030
dfn-cert: DFN-CERT-2018-2560
dfn-cert: DFN-CERT-2018-2559
dfn-cert: DFN-CERT-2018-2557
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2512
dfn-cert: DFN-CERT-2018-2465
dfn-cert: DFN-CERT-2018-2450
dfn-cert: DFN-CERT-2018-2342
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-2304
dfn-cert: DFN-CERT-2018-2091
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0592
```

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.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:7.4.052-1ubuntu3.1
Fixed version:      >=vim-tiny-2:7.4.052-1ubuntu3.1+esm10
```

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, 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: `2023-06-13T10:40:18Z`

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-2023-1347
dfn-cert: DFN-CERT-2023-1159
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3127-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux' package(s) announced via the USN-3127-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.101.109
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that the compression handling code in the Advanced Linux Sound Architecture (ALSA) subsystem in the Linux kernel did not properly check for an integer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2014-9904)
Kirill A. Shutemov discovered that memory manager in the Linux kernel did not properly handle anonymous pages. A local attacker could use this to cause a denial of service or possibly gain administrative privileges. (CVE-2015-3288)
Vitaly Kuznetsov discovered that the Linux kernel did not properly suppress hugetlbfs support in X86 paravirtualized guests. An attacker in the guest OS could cause a denial of service (guest system crash). (CVE-2016-3961)
Ondrej Kozina discovered that the keyring interface in the Linux kernel contained a buffer overflow when displaying timeout events via the /proc/keys interface. A local attacker could use this to cause a denial of service (system crash). (CVE-2016-7042)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3127-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2016.3127.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3127-1
cve: CVE-2014-9904
cve: CVE-2015-3288
cve: CVE-2016-3961
cve: CVE-2016-7042
advisory_id: USN-3127-1
cert-bund: WID-SEC-2022-1345
cert-bund: CB-K17/1520
cert-bund: CB-K17/1484
cert-bund: CB-K17/1286
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0826
cert-bund: CB-K17/0697
cert-bund: CB-K17/0484
cert-bund: CB-K17/0297
cert-bund: CB-K17/0277
cert-bund: CB-K17/0168
cert-bund: CB-K17/0088
cert-bund: CB-K17/0063
cert-bund: CB-K17/0013
cert-bund: CB-K17/0011
cert-bund: CB-K17/0001
cert-bund: CB-K16/1999
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
cert-bund: CB-K16/1900
cert-bund: CB-K16/1878
cert-bund: CB-K16/1869
cert-bund: CB-K16/1843
cert-bund: CB-K16/1757
cert-bund: CB-K16/1627
cert-bund: CB-K16/1292
cert-bund: CB-K16/1277
cert-bund: CB-K16/1229
cert-bund: CB-K16/1176
cert-bund: CB-K16/1174
cert-bund: CB-K16/1172
cert-bund: CB-K16/1013
cert-bund: CB-K16/0988
cert-bund: CB-K16/0880
cert-bund: CB-K16/0607
cert-bund: CB-K16/0566
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0496
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2017-0063
dfn-cert: DFN-CERT-2017-0011
dfn-cert: DFN-CERT-2017-0010
dfn-cert: DFN-CERT-2017-0001
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2026
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-2024
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-1984
dfn-cert: DFN-CERT-2016-1975
dfn-cert: DFN-CERT-2016-1948
dfn-cert: DFN-CERT-2016-1863
dfn-cert: DFN-CERT-2016-1731
dfn-cert: DFN-CERT-2016-1376
dfn-cert: DFN-CERT-2016-1360
dfn-cert: DFN-CERT-2016-1307
dfn-cert: DFN-CERT-2016-1249
dfn-cert: DFN-CERT-2016-1246
dfn-cert: DFN-CERT-2016-1245
dfn-cert: DFN-CERT-2016-1078
dfn-cert: DFN-CERT-2016-1049
dfn-cert: DFN-CERT-2016-0936
dfn-cert: DFN-CERT-2016-0652
dfn-cert: DFN-CERT-2016-0615
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4672-1)

Summary
The remote host is missing an update for the 'unzip' package(s) announced via the USN-4672-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   unzip
Installed version:    unzip-6.0-9ubuntu1.5
Fixed version:      >=unzip-6.0-9ubuntu1.6
```

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

Affected Software/OS
'unzip' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
Rene Freingruber discovered that unzip incorrectly handled certain specially crafted password protected ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. (CVE-2018-1000035)

. . . continues on next page . . .

. . . continued from previous page . . .

Antonio Carista discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. (CVE-2018-18384)
It was discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause resource consumption, resulting in a denial of service. (CVE-2019-13232)
Martin Carpenter discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2014-9913)
Alexis Vanden Eijnde discovered that unzip incorrectly handled certain specially crafted ZIP archives. If a user or automated system using unzip were tricked into opening a specially crafted zip file, an attacker could exploit this to cause a crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM and Ubuntu 16.04 LTS. (CVE-2016-9844)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4672-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4672.1
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4672-1
cve: CVE-2014-9913
cve: CVE-2016-9844
cve: CVE-2018-1000035
cve: CVE-2018-18384
cve: CVE-2019-13232
advisory_id: USN-4672-1
cert-bund: CB-K20/1049
cert-bund: CB-K18/0306
cert-bund: CB-K17/0410
cert-bund: CB-K16/1965
dfn-cert: DFN-CERT-2020-2751
dfn-cert: DFN-CERT-2019-1362
dfn-cert: DFN-CERT-2019-0578
dfn-cert: DFN-CERT-2018-2003
dfn-cert: DFN-CERT-2018-1311
dfn-cert: DFN-CERT-2018-0330
dfn-cert: DFN-CERT-2017-0411
dfn-cert: DFN-CERT-2016-2075
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4135-2)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-lts-trusty, linux-lts-xenial' package(s) announced via the USN-4135-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.173.184
```

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-lts-trusty, linux-lts-xenial' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
Peter Pi discovered a buffer overflow in the virtio network backend (vhost_net) implementation in the Linux kernel. An attacker in a guest may be able to use this to cause a denial of service (host OS crash) or possibly execute arbitrary code in the host OS. (CVE-2019-14835)
It was discovered that the Linux kernel on PowerPC architectures did not properly handle Facility Unavailable exceptions in some situations. A local attacker could use this to expose sensitive information. (CVE-2019-15030)
It was discovered that the Linux kernel on PowerPC architectures did not properly handle exceptions on interrupts in some situations. A local attacker could use this to expose sensitive information. (CVE-2019-15031)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4135-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4135.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4135-2
cve: CVE-2019-14835
cve: CVE-2019-15030
cve: CVE-2019-15031
advisory_id: USN-4135-2
cert-bund: CB-K19/0820
cert-bund: CB-K19/0818
dfn-cert: DFN-CERT-2020-0796
dfn-cert: DFN-CERT-2020-0726
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0481
dfn-cert: DFN-CERT-2020-0158
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2582
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-2421
dfn-cert: DFN-CERT-2019-2402
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2388
dfn-cert: DFN-CERT-2019-2273
dfn-cert: DFN-CERT-2019-2262
dfn-cert: DFN-CERT-2019-2217
dfn-cert: DFN-CERT-2019-2133
dfn-cert: DFN-CERT-2019-2132
dfn-cert: DFN-CERT-2019-2127
dfn-cert: DFN-CERT-2019-2109
dfn-cert: DFN-CERT-2019-2108
dfn-cert: DFN-CERT-2019-2007
dfn-cert: DFN-CERT-2019-1994
dfn-cert: DFN-CERT-2019-1993
dfn-cert: DFN-CERT-2019-1969
dfn-cert: DFN-CERT-2019-1963
dfn-cert: DFN-CERT-2019-1952
dfn-cert: DFN-CERT-2019-1946
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4580-1)

Summary
The remote host is missing an update for the 'linux, linux-lts-trusty' package(s) announced via the USN-4580-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.182.191
```

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

Affected Software/OS
'linux, linux-lts-trusty' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Hadar Manor discovered that the DCCP protocol implementation in the Linux kernel improperly handled socket reuse, 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.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4580-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4580.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4580-1
cve: CVE-2020-16119
advisory_id: USN-4580-1
cert-bund: WID-SEC-2022-1762
cert-bund: CB-K20/0976
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-2915
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-2021-2637
dfn-cert: DFN-CERT-2021-2171
dfn-cert: DFN-CERT-2021-2161
dfn-cert: DFN-CERT-2021-2095
dfn-cert: DFN-CERT-2021-2011
dfn-cert: DFN-CERT-2020-2253
dfn-cert: DFN-CERT-2020-2249
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3406-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-3406-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.129.138
```

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 14.04.

Vulnerability Insight
It was discovered that an out of bounds read vulnerability existed in the associative array implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2016-7914)
It was discovered that a NULL pointer dereference existed in the Direct Rendering Manager (DRM) driver for VMWare devices in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-7261)
It was discovered that the USB Cypress HID drivers for the Linux kernel did not properly validate reported information from the device. An attacker with physical access could use this to expose sensitive information (kernel memory). (CVE-2017-7273)
A reference count bug was discovered in the Linux kernel ipx protocol stack. A local attacker could exploit this flaw to cause a denial of service or possibly other unspecified problems. (CVE-2017-7487)
Huang Weller discovered that the ext4 filesystem implementation in the Linux kernel mishandled a needs-flushing-before-commit list. A local attacker could use this to expose sensitive information. (CVE-2017-7495)
It was discovered that an information leak existed in the set_mempolicy and mbind compat syscalls in the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2017-7616)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3406-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3406.1
Version used: `2023-02-16T04:10:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-3406-1
cve: CVE-2016-7914
cve: CVE-2017-7261
cve: CVE-2017-7273
cve: CVE-2017-7487
cve: CVE-2017-7495
cve: CVE-2017-7616
advisory_id: USN-3406-1
cert-bund: CB-K18/0184
cert-bund: CB-K17/2141
cert-bund: CB-K17/1849
cert-bund: CB-K17/1584
cert-bund: CB-K17/1530
cert-bund: CB-K17/1505
cert-bund: CB-K17/1491
cert-bund: CB-K17/1484
```

. . . continues on next page . . .

... continued from previous page ...

```
cert-bund: CB-K17/1449
cert-bund: CB-K17/1286
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1226
cert-bund: CB-K17/1178
cert-bund: CB-K17/1101
cert-bund: CB-K17/1025
cert-bund: CB-K17/1020
cert-bund: CB-K17/0961
cert-bund: CB-K17/0866
cert-bund: CB-K17/0843
cert-bund: CB-K17/0836
cert-bund: CB-K17/0826
cert-bund: CB-K17/0812
cert-bund: CB-K17/0773
cert-bund: CB-K17/0764
cert-bund: CB-K17/0719
cert-bund: CB-K17/0636
cert-bund: CB-K17/0545
cert-bund: CB-K17/0534
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0212
cert-bund: CB-K16/1911
cert-bund: CB-K16/1740
cert-bund: CB-K16/1739
dfn-cert: DFN-CERT-2020-0974
dfn-cert: DFN-CERT-2019-2168
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0203
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-1404
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1337
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1570
dfn-cert: DFN-CERT-2017-1556
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1513
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1317
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-1219
dfn-cert: DFN-CERT-2017-1139
dfn-cert: DFN-CERT-2017-1062
dfn-cert: DFN-CERT-2017-1057
dfn-cert: DFN-CERT-2017-0995
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0863
dfn-cert: DFN-CERT-2017-0855
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0799
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0743
dfn-cert: DFN-CERT-2017-0657
dfn-cert: DFN-CERT-2017-0562
dfn-cert: DFN-CERT-2017-0546
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2016-1843
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3386-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3386-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.128.137
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

Andrey Konovalov discovered a race condition in the UDP Fragmentation Offload (UFO) code in the Linux kernel. A local attacker could use this to cause a denial of service or execute arbitrary code. (CVE-2017-1000112)
Andrey Konovalov discovered a race condition in AF_PACKET socket option handling code in the Linux kernel. A local unprivileged attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2017-1000111)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3386-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3386.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3386-1
cve: CVE-2017-1000111
cve: CVE-2017-1000112
advisory_id: USN-3386-1
cert-bund: CB-K18/0471
cert-bund: CB-K18/0462
cert-bund: CB-K18/0398
cert-bund: CB-K18/0184
cert-bund: CB-K18/0066
cert-bund: CB-K17/2169
cert-bund: CB-K17/2144
cert-bund: CB-K17/2141
cert-bund: CB-K17/2124
cert-bund: CB-K17/1952
cert-bund: CB-K17/1908
cert-bund: CB-K17/1867
cert-bund: CB-K17/1804
cert-bund: CB-K17/1792
cert-bund: CB-K17/1776
cert-bund: CB-K17/1770
cert-bund: CB-K17/1696
cert-bund: CB-K17/1607
cert-bund: CB-K17/1584
cert-bund: CB-K17/1546
cert-bund: CB-K17/1452
cert-bund: CB-K17/1418
cert-bund: CB-K17/1381
cert-bund: CB-K17/1357
dfn-cert: DFN-CERT-2019-2614
dfn-cert: DFN-CERT-2019-1551
dfn-cert: DFN-CERT-2018-0509
dfn-cert: DFN-CERT-2018-0500
dfn-cert: DFN-CERT-2018-0427
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2042
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1887
dfn-cert: DFN-CERT-2017-1867
dfn-cert: DFN-CERT-2017-1852
dfn-cert: DFN-CERT-2017-1851
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1617
dfn-cert: DFN-CERT-2017-1518
dfn-cert: DFN-CERT-2017-1479
dfn-cert: DFN-CERT-2017-1444
dfn-cert: DFN-CERT-2017-1421
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3381-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3381-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.126.136
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Peter Pi discovered that the colormap handling for frame buffer devices in the Linux kernel contained an integer overflow. A local attacker could use this to disclose sensitive information (kernel memory). (CVE-2016-8405)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the Linux kernel did not properly restrict RLIMIT_STACK size. A local attacker could use this in conjunction with another vulnerability to possibly execute arbitrary code. (CVE-2017-1000365)

It was discovered that SELinux in the Linux kernel did not properly handle empty writes to /proc/pid/attr. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-2618)

Shi Lei discovered that the RxRPC Kerberos 5 ticket handling code in the Linux kernel did not properly verify metadata. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-7482)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3381-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2017.3381.1

Version used: `2023-02-16T04:10:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-3381-1
cve: CVE-2016-8405
cve: CVE-2017-1000365
cve: CVE-2017-2618
cve: CVE-2017-7482
advisory_id: USN-3381-1
cert-bund: CB-K18/0364
cert-bund: CB-K18/0184
cert-bund: CB-K18/0165
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
cert-bund: CB-K17/2169
cert-bund: CB-K17/2141
cert-bund: CB-K17/2125
cert-bund: CB-K17/2124
cert-bund: CB-K17/1940
cert-bund: CB-K17/1908
cert-bund: CB-K17/1867
cert-bund: CB-K17/1849
cert-bund: CB-K17/1719
cert-bund: CB-K17/1602
cert-bund: CB-K17/1584
cert-bund: CB-K17/1530
cert-bund: CB-K17/1484
cert-bund: CB-K17/1443
cert-bund: CB-K17/1408
cert-bund: CB-K17/1331
cert-bund: CB-K17/1325
cert-bund: CB-K17/1317
cert-bund: CB-K17/1267
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1226
cert-bund: CB-K17/1178
cert-bund: CB-K17/1144
cert-bund: CB-K17/1029
cert-bund: CB-K17/0628
cert-bund: CB-K17/0326
cert-bund: CB-K16/1876
dfn-cert: DFN-CERT-2019-0607
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0392
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2017-2314
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-2224
dfn-cert: DFN-CERT-2017-2023
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1801
dfn-cert: DFN-CERT-2017-1669
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1505
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1380
dfn-cert: DFN-CERT-2017-1376
dfn-cert: DFN-CERT-2017-1367
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1271
dfn-cert: DFN-CERT-2017-1219
dfn-cert: DFN-CERT-2017-1183
dfn-cert: DFN-CERT-2017-1056
dfn-cert: DFN-CERT-2017-0649
dfn-cert: DFN-CERT-2017-0331
dfn-cert: DFN-CERT-2016-1981
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3775-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3775-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.160.170
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that the paravirtualization implementation in the Linux kernel did not properly handle some indirect calls, reducing the effectiveness of Spectre v2 mitigations for paravirtual guests. A local attacker could use this to expose sensitive information. (CVE-2018-15594)
It was discovered that microprocessors utilizing speculative execution and prediction of return addresses via Return Stack Buffer (RSB) may allow unauthorized memory reads via sidechannel attacks. An attacker could use this to expose sensitive information. (CVE-2018-15572)
It was discovered that an integer overflow vulnerability existed in the Linux kernel when loading an executable to run. A local attacker could use this to gain administrative privileges. (CVE-2018-14634)
It was discovered that a stack-based buffer overflow existed in the iSCSI target implementation of the Linux kernel. A remote attacker could use this to cause a denial of service (system crash). (CVE-2018-14633)
It was discovered that a memory leak existed in the IRDA subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (kernel memory exhaustion). (CVE-2018-6554)
It was discovered that a use-after-free vulnerability existed in the IRDA 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-2018-6555)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3775-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3775.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-3775-1`
`cve: CVE-2018-14633`

... continues on next page ...

. . . continued from previous page . . .

```
cve: CVE-2018-14634
cve: CVE-2018-15572
cve: CVE-2018-15594
cve: CVE-2018-6554
cve: CVE-2018-6555
advisory_id: USN-3775-1
cert-bund: CB-K18/0957
cert-bund: CB-K18/0951
cert-bund: CB-K18/0942
cert-bund: CB-K18/0936
cert-bund: CB-K18/0897
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1554
dfn-cert: DFN-CERT-2019-1214
dfn-cert: DFN-CERT-2019-1132
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1005
dfn-cert: DFN-CERT-2019-0658
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0115
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2018-2458
dfn-cert: DFN-CERT-2018-2421
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2398
dfn-cert: DFN-CERT-2018-2366
dfn-cert: DFN-CERT-2018-2359
dfn-cert: DFN-CERT-2018-2335
dfn-cert: DFN-CERT-2018-2318
dfn-cert: DFN-CERT-2018-2304
dfn-cert: DFN-CERT-2018-2294
dfn-cert: DFN-CERT-2018-2280
dfn-cert: DFN-CERT-2018-2252
dfn-cert: DFN-CERT-2018-2167
dfn-cert: DFN-CERT-2018-2129
dfn-cert: DFN-CERT-2018-2118
dfn-cert: DFN-CERT-2018-2117
dfn-cert: DFN-CERT-2018-2099
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2063
dfn-cert: DFN-CERT-2018-2060
dfn-cert: DFN-CERT-2018-2050
dfn-cert: DFN-CERT-2018-2039
dfn-cert: DFN-CERT-2018-2029
dfn-cert: DFN-CERT-2018-1997
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1995
dfn-cert: DFN-CERT-2018-1990
dfn-cert: DFN-CERT-2018-1967
dfn-cert: DFN-CERT-2018-1966
dfn-cert: DFN-CERT-2018-1963
dfn-cert: DFN-CERT-2018-1962
dfn-cert: DFN-CERT-2018-1946
dfn-cert: DFN-CERT-2018-1940
dfn-cert: DFN-CERT-2018-1905
dfn-cert: DFN-CERT-2018-1870
dfn-cert: DFN-CERT-2018-1789
dfn-cert: DFN-CERT-2018-1748
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3343-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3343-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.123.133
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN 3335-1 fixed a vulnerability in the Linux kernel. However, that fix introduced regressions for some Java applications. This update addresses the issue. We apologize for the inconvenience.
It was discovered that a use-after-free vulnerability in the core voltage regulator driver of the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2014-9940)
It was discovered that a buffer overflow existed in the trace subsystem in the Linux kernel. A privileged local attacker could use this to execute arbitrary code. (CVE-2017-0605)
Roee Hay discovered that the parallel port printer driver in the Linux kernel did not properly bounds check passed arguments. A local attacker with write access to the kernel command line arguments could use this to execute arbitrary code. (CVE-2017-1000363)
Li Qiang discovered that an integer overflow vulnerability existed in the Direct Rendering Manager (DRM) driver for VMWare devices in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-7294)

. . . continues on next page . . .

... continued from previous page ...

It was discovered that a double-free vulnerability existed in the IPv4 stack of the Linux kernel. An attacker could use this to cause a denial of service (system crash). (CVE-2017-8890)
Andrey Konovalov discovered an IPv6 out-of-bounds read error in the Linux kernel's IPv6 stack. A local attacker could cause a denial of service or potentially other unspecified problems. (CVE-2017-9074)
Andrey Konovalov discovered a flaw in the handling of inheritance in the Linux kernel's IPv6 stack. A local user could exploit this issue to cause a denial of service or possibly other unspecified problems. (CVE-2017-9075)
It was discovered that dccp v6 in the Linux kernel mishandled inheritance. A local attacker could exploit this issue to cause a denial of service or potentially other unspecified problems. (CVE-2017-9076)
It was discovered that the transmission control protocol (tcp) v6 in the Linux kernel mishandled inheritance. A local attacker could exploit this issue to cause a denial of service or potentially other unspecified problems. (CVE-2017-9077)
It was discovered that the IPv6 stack in the Linux kernel was performing its over write consistency check after the data was actually overwritten. A local attacker could exploit this flaw to cause a denial of service (system crash). (CVE-2017-9242)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3343-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3343.1
Version used: `2023-02-27T04:10:43Z`

References

```
url: https://ubuntu.com/security/notices/USN-3343-1
url: https://www.ubuntu.com/usn/usn-3335-1
url: https://launchpad.net/bugs/1699772
cve: CVE-2014-9940
cve: CVE-2017-0605
cve: CVE-2017-1000363
cve: CVE-2017-7294
cve: CVE-2017-8890
cve: CVE-2017-9074
cve: CVE-2017-9075
cve: CVE-2017-9076
cve: CVE-2017-9077
cve: CVE-2017-9242
advisory_id: USN-3343-1
cert-bund: CB-K18/0471
cert-bund: CB-K18/0364
cert-bund: CB-K18/0184
cert-bund: CB-K18/0166
cert-bund: CB-K18/0022
cert-bund: CB-K17/2141
cert-bund: CB-K17/2124
cert-bund: CB-K17/1905
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K17/1892
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1849
cert-bund: CB-K17/1830
cert-bund: CB-K17/1770
cert-bund: CB-K17/1649
cert-bund: CB-K17/1584
cert-bund: CB-K17/1546
cert-bund: CB-K17/1530
cert-bund: CB-K17/1520
cert-bund: CB-K17/1505
cert-bund: CB-K17/1491
cert-bund: CB-K17/1484
cert-bund: CB-K17/1419
cert-bund: CB-K17/1408
cert-bund: CB-K17/1404
cert-bund: CB-K17/1323
cert-bund: CB-K17/1286
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1225
cert-bund: CB-K17/1178
cert-bund: CB-K17/1102
cert-bund: CB-K17/1101
cert-bund: CB-K17/1034
cert-bund: CB-K17/1025
cert-bund: CB-K17/1020
cert-bund: CB-K17/0961
cert-bund: CB-K17/0941
cert-bund: CB-K17/0923
cert-bund: CB-K17/0885
cert-bund: CB-K17/0876
cert-bund: CB-K17/0866
cert-bund: CB-K17/0836
cert-bund: CB-K17/0826
cert-bund: CB-K17/0825
cert-bund: CB-K17/0812
cert-bund: CB-K17/0792
cert-bund: CB-K17/0773
cert-bund: CB-K17/0764
cert-bund: CB-K17/0727
cert-bund: CB-K17/0719
cert-bund: CB-K17/0678
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-0932
dfn-cert: DFN-CERT-2018-0931
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0509
dfn-cert: DFN-CERT-2018-0392
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0182
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-1989
dfn-cert: DFN-CERT-2017-1972
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1913
dfn-cert: DFN-CERT-2017-1851
dfn-cert: DFN-CERT-2017-1726
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1617
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1570
dfn-cert: DFN-CERT-2017-1556
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1477
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1467
dfn-cert: DFN-CERT-2017-1372
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1268
dfn-cert: DFN-CERT-2017-1219
dfn-cert: DFN-CERT-2017-1140
dfn-cert: DFN-CERT-2017-1139
dfn-cert: DFN-CERT-2017-1070
dfn-cert: DFN-CERT-2017-1062
dfn-cert: DFN-CERT-2017-1057
dfn-cert: DFN-CERT-2017-0995
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0956
dfn-cert: DFN-CERT-2017-0914
dfn-cert: DFN-CERT-2017-0900
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0863
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0850
dfn-cert: DFN-CERT-2017-0838
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0820
dfn-cert: DFN-CERT-2017-0799
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0743
dfn-cert: DFN-CERT-2017-0742
dfn-cert: DFN-CERT-2017-0699
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3256-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon, linux-ti-omap4' package(s) announced via the USN-3256-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.116.126
```

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

Affected Software/OS
'linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon, linux-ti-omap4' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 16.10.

Vulnerability Insight
Andrey Konovalov discovered that the AF_PACKET implementation in the Linux kernel did not properly validate certain block-size data. A local attacker could 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-3256-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3256.1
Version used: `2023-02-16T04:10:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-3256-1
cve: CVE-2017-7308
advisory_id: USN-3256-1
cert-bund: CB-K18/0184
cert-bund: CB-K17/2141
cert-bund: CB-K17/1869
cert-bund: CB-K17/1584
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1484
cert-bund: CB-K17/1267
cert-bund: CB-K17/1261
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/1101
cert-bund: CB-K17/0924
cert-bund: CB-K17/0923
cert-bund: CB-K17/0884
cert-bund: CB-K17/0866
cert-bund: CB-K17/0826
cert-bund: CB-K17/0825
cert-bund: CB-K17/0812
cert-bund: CB-K17/0773
cert-bund: CB-K17/0764
cert-bund: CB-K17/0719
cert-bund: CB-K17/0678
cert-bund: CB-K17/0636
cert-bund: CB-K17/0563
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-1139
dfn-cert: DFN-CERT-2017-0956
dfn-cert: DFN-CERT-2017-0955
dfn-cert: DFN-CERT-2017-0912
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0850
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0799
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0743
dfn-cert: DFN-CERT-2017-0699
dfn-cert: DFN-CERT-2017-0657
dfn-cert: DFN-CERT-2017-0582
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3207-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3207-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.110.118
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that a use-after-free vulnerability existed in the block device layer of the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly gain administrative privileges. (CVE-2016-7910)
Dmitry Vyukov discovered a use-after-free vulnerability in the sys_ioprio_get() function in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly gain administrative privileges. (CVE-2016-7911)
Andrey Konovalov discovered a use-after-free vulnerability in the DCCP implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly gain administrative privileges. (CVE-2017-6074)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3207-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3207.1
Version used: `2023-02-13T04:10:52Z`

References

```
url: https://ubuntu.com/security/notices/USN-3207-1
cve: CVE-2016-7910
cve: CVE-2016-7911
cve: CVE-2017-6074
advisory_id: USN-3207-1
cert-bund: WID-SEC-2022-2099
cert-bund: CB-K17/1584
cert-bund: CB-K17/1484
cert-bund: CB-K17/1267
cert-bund: CB-K17/1134
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1133
cert-bund: CB-K17/0884
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
cert-bund: CB-K17/0838
cert-bund: CB-K17/0826
cert-bund: CB-K17/0812
cert-bund: CB-K17/0764
cert-bund: CB-K17/0697
cert-bund: CB-K17/0648
cert-bund: CB-K17/0647
cert-bund: CB-K17/0646
cert-bund: CB-K17/0628
cert-bund: CB-K17/0605
cert-bund: CB-K17/0552
cert-bund: CB-K17/0335
cert-bund: CB-K17/0332
cert-bund: CB-K17/0326
cert-bund: CB-K17/0325
cert-bund: CB-K17/0324
cert-bund: CB-K17/0317
cert-bund: CB-K17/0297
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0168
cert-bund: CB-K16/1911
cert-bund: CB-K16/1740
cert-bund: CB-K16/1739
dfn-cert: DFN-CERT-2021-2161
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0912
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0666
dfn-cert: DFN-CERT-2017-0665
dfn-cert: DFN-CERT-2017-0664
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0649
dfn-cert: DFN-CERT-2017-0626
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0342
dfn-cert: DFN-CERT-2017-0338
dfn-cert: DFN-CERT-2017-0331
dfn-cert: DFN-CERT-2017-0328
dfn-cert: DFN-CERT-2017-0327
dfn-cert: DFN-CERT-2017-0322
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2016-1843
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-6166-2)

Summary
The remote host is missing an update for the 'libcap2' package(s) announced via the USN-6166-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libcap2
Installed version:    libcap2-1:2.24-0ubuntu2
Fixed version:      >=libcap2-1:2.24-0ubuntu2+esm1
Vulnerable package:   libcap2-bin
Installed version:    libcap2-bin-1:2.24-0ubuntu2
Fixed version:      >=libcap2-bin-1:2.24-0ubuntu2+esm1
```

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

Affected Software/OS
'libcap2' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
USN-6166-1 fixed a vulnerability in libcap2. This update provides the corresponding update for Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

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-6166-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6166.2
Version used: `2023-06-23T04:09:37Z`

References
```
url: https://ubuntu.com/security/notices/USN-6166-2
cve: CVE-2023-2603
advisory_id: USN-6166-2
dfn-cert: DFN-CERT-2023-1380
```

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

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

Vulnerability Detection Result
```
Vulnerable package:   vim-tiny
Installed version:    vim-tiny-2:7.4.052-1ubuntu3.1
Fixed version:      >=vim-tiny-2:7.4.052-1ubuntu3.1+esm7
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

References

```
url: https://ubuntu.com/security/notices/USN-5963-1
cve: CVE-2022-47024
cve: CVE-2023-0049
cve: CVE-2023-0051
cve: CVE-2023-0054
cve: CVE-2023-0288
cve: CVE-2023-0433
cve: CVE-2023-1170
cve: CVE-2023-1175
cve: CVE-2023-1264
advisory_id: USN-5963-1
cert-bund: WID-SEC-2023-1542
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-2023-1347
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-5464-1)

Summary
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:    e2fsprogs-1.42.9-3ubuntu1.2
Fixed version:      >=e2fsprogs-1.42.9-3ubuntu1.3+esm3
```

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: `2022-09-13T14:14:11Z`

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-2022-1091
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4172-2)

Summary
The remote host is missing an update for the 'file' package(s) announced via the USN-4172-2 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   file
Installed version:    file-1:5.14-2ubuntu3.4
Fixed version:      >=file-1:5.14-2ubuntu3.4+esm1
Vulnerable package:   libmagic1
Installed version:    libmagic1-1:5.14-2ubuntu3.4
Fixed version:      >=libmagic1-1:5.14-2ubuntu3.4+esm1
```

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

Affected Software/OS
'file' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4172-1 fixed a vulnerability in file. This update provides the corresponding update for Ubuntu 12.04 ESM Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that file incorrectly handled certain malformed files. 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-4172-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4172.2
Version used: `2022-11-14T04:23:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-4172-2
cve: CVE-2019-18218
advisory_id: USN-4172-2
cert-bund: WID-SEC-2022-0571
cert-bund: CB-K21/1164
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-1509
dfn-cert: DFN-CERT-2020-1376
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2215
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3968-3)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'sudo' package(s) announced via the USN-3968-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm5
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'sudo' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-3968-1 fixed several vulnerabilities in Sudo. This update provides the corresponding update for Ubuntu 14.04 ESM.

Original advisory details:

Florian Weimer discovered that Sudo incorrectly handled the noexec restriction when used with certain applications. A local attacker could possibly use this issue to bypass configured restrictions and execute arbitrary commands. (CVE-2016-7076, CVE-2016-7032)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3968-3)`

OID:1.3.6.1.4.1.25623.1.1.12.2020.3968.3

Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-3968-3
cve: CVE-2016-7032
cve: CVE-2016-7076
advisory_id: USN-3968-3
cert-bund: CB-K16/1681
dfn-cert: DFN-CERT-2019-0903
dfn-cert: DFN-CERT-2016-1775
```

High (CVSS: 7.8)

NVT: Ubuntu: Security Advisory (USN-4263-2)

Summary

The remote host is missing an update for the 'sudo' package(s) announced via the USN-4263-2 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm3
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'sudo' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4263-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.

Original advisory details:

Joe Vennix discovered that Sudo incorrectly handled memory operations when the pwfeedback option is enabled. A local attacker could possibly use this issue to obtain unintended access to the administrator account.

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-4263-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2020.4263.2

Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4263-2
cve: CVE-2019-18634
advisory_id: USN-4263-2
cert-bund: CB-K20/0109
cert-bund: CB-K20/0092
cert-bund: CB-K20/0081
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0095
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-0443
dfn-cert: DFN-CERT-2020-0308
dfn-cert: DFN-CERT-2020-0220
dfn-cert: DFN-CERT-2020-0193
```

High (CVSS: 7.8)

NVT: Ubuntu: Security Advisory (USN-4360-4)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'json-c' package(s) announced via the USN-4360-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjson-c2
Installed version:    libjson-c2-0.11-3ubuntu1.2
Fixed version:      >=libjson-c2-0.11-3ubuntu1.2+esm3
Vulnerable package:   libjson0
Installed version:    libjson0-0.11-3ubuntu1.2
Fixed version:      >=libjson0-0.11-3ubuntu1.2+esm3
```

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

Affected Software/OS
'json-c' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
USN-4360-1 fixed a vulnerability in json-c. The security fix introduced a memory leak that was reverted in USN-4360-2 and USN-4360-3. This update provides the correct fix update for CVE-2020-12762.
Original advisory details:
It was discovered that json-c incorrectly handled certain JSON 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-4360-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4360.4
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4360-4
cve: CVE-2020-12762
advisory_id: USN-4360-4
cert-bund: WID-SEC-2022-0571
cert-bund: CB-K21/1164
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2020-1533
dfn-cert: DFN-CERT-2020-1039
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4360-1)

Summary
The remote host is missing an update for the 'json-c' package(s) announced via the USN-4360-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjson-c2
Installed version:    libjson-c2-0.11-3ubuntu1.2
Fixed version:      >=libjson-c2-0.11-3ubuntu1.2+esm1
Vulnerable package:   libjson0
Installed version:    libjson0-0.11-3ubuntu1.2
Fixed version:      >=libjson0-0.11-3ubuntu1.2+esm1
```

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

Affected Software/OS
'json-c' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
It was discovered that json-c incorrectly handled certain JSON 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-4360-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4360.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4360-1
cve: CVE-2020-12762
advisory_id: USN-4360-1
cert-bund: WID-SEC-2022-0571
cert-bund: CB-K21/1164
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2020-1533
dfn-cert: DFN-CERT-2020-1039
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-4705-2)

. . . 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-4705-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm6
```

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

Affected Software/OS
'sudo' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4705-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Sudo incorrectly handled memory when parsing command lines. A local attacker could possibly use this issue to obtain unintended access to the administrator account. (CVE-2021-3156)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4705-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4705.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4705-2
cve: CVE-2021-3156
advisory_id: USN-4705-2
cert-bund: WID-SEC-2023-0066
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-0623
cert-bund: CB-K22/0130
cert-bund: CB-K21/0161
cert-bund: CB-K21/0092
dfn-cert: DFN-CERT-2022-0224
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0781
dfn-cert: DFN-CERT-2021-0299
dfn-cert: DFN-CERT-2021-0249
dfn-cert: DFN-CERT-2021-0202
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-0181
dfn-cert: DFN-CERT-2021-0180
dfn-cert: DFN-CERT-2021-0178
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-5811-3)

Summary
The remote host is missing an update for the 'sudo' package(s) announced via the USN-5811-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   sudo
Installed version:    sudo-1.8.9p5-1ubuntu1.4
Fixed version:      >=sudo-1.8.9p5-1ubuntu1.5+esm7
```

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

Affected Software/OS
'sudo' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-5811-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
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)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5811-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5811.3
Version used: `2023-01-31T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-5811-3
cve: CVE-2023-22809
advisory_id: USN-5811-3
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-0151
dfn-cert: DFN-CERT-2023-0662
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2023-0423
dfn-cert: DFN-CERT-2023-0129
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3641-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-euclid, linux-gcp, linux-hwe, linux-kvm, linux-lts-xenial, linux-oem, linux-raspi2, linux-snapdragon' package(s) announced via the USN-3641-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.147.157
```

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

Affected Software/OS
'linux, linux-aws, linux-azure, linux-euclid, linux-gcp, linux-hwe, linux-kvm, linux-lts-xenial, linux-oem, linux-raspi2, linux-snapdragon' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 17.10.

Vulnerability Insight
Nick Peterson discovered that the Linux kernel did not properly handle debug exceptions following a MOV/POP to SS instruction. A local attacker could use this to cause a denial of service (system crash). This issue only affected the amd64 architecture. (CVE-2018-8897)
Andy Lutomirski discovered that the KVM subsystem of the Linux kernel did not properly emulate the ICEBP instruction following a MOV/POP to SS instruction. A local attacker in a KVM virtual machine could use this to cause a denial of service (guest VM crash) or possibly escalate privileges inside of the virtual machine. This issue only affected the i386 and amd64 architectures. (CVE-2018-1087)
Andy Lutomirski discovered that the Linux kernel did not properly perform error handling on virtualized debug registers. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-1000199)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3641-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3641.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-3641-1
cve: CVE-2018-1000199
cve: CVE-2018-1087
cve: CVE-2018-8897
advisory_id: USN-3641-1
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K19/0774
cert-bund: CB-K19/0014
cert-bund: CB-K18/0698
cert-bund: CB-K18/0659
cert-bund: CB-K18/0654
cert-bund: CB-K18/0653
cert-bund: CB-K18/0652
cert-bund: CB-K18/0635
cert-bund: CB-K18/0630
dfn-cert: DFN-CERT-2020-1929
dfn-cert: DFN-CERT-2020-1921
dfn-cert: DFN-CERT-2020-1739
dfn-cert: DFN-CERT-2020-1365
dfn-cert: DFN-CERT-2020-1319
dfn-cert: DFN-CERT-2020-1318
dfn-cert: DFN-CERT-2020-1277
dfn-cert: DFN-CERT-2020-1247
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2309
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1279
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1170
dfn-cert: DFN-CERT-2018-1151
dfn-cert: DFN-CERT-2018-1105
dfn-cert: DFN-CERT-2018-1072
dfn-cert: DFN-CERT-2018-1059
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0992
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0936
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0928
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0911
dfn-cert: DFN-CERT-2018-0896
dfn-cert: DFN-CERT-2018-0895
dfn-cert: DFN-CERT-2018-0890
dfn-cert: DFN-CERT-2018-0889
dfn-cert: DFN-CERT-2018-0888
dfn-cert: DFN-CERT-2018-0887
dfn-cert: DFN-CERT-2018-0886
dfn-cert: DFN-CERT-2018-0885
dfn-cert: DFN-CERT-2018-0884
dfn-cert: DFN-CERT-2018-0883
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0881
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0869
dfn-cert: DFN-CERT-2018-0868
dfn-cert: DFN-CERT-2018-0865
dfn-cert: DFN-CERT-2018-0823
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0785
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3674-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3674-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.151.161
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that the netfilter subsystem of the Linux kernel did not properly validate ebtables offsets. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2018-1068)

It was discovered that a NULL pointer dereference existed in the RDS (Reliable Datagram Sockets) protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2018-7492)

Eyal Itkin discovered that the USB displaylink video adapter driver in the Linux kernel did not properly validate mmap offsets sent from userspace. A local attacker could use this to expose sensitive information (kernel memory) or possibly execute arbitrary code. (CVE-2018-8781)

Xingyuan Lin discovered that a out-of-bounds read existed in the USB Video Class (UVC) driver of the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2017-0627)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3674-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2018.3674.1

Version used: `2023-02-27T04:10:43Z`

References

```
url: https://ubuntu.com/security/notices/USN-3674-1
cve: CVE-2017-0627
cve: CVE-2018-1068
cve: CVE-2018-7492
cve: CVE-2018-8781
advisory_id: USN-3674-1
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K18/0839
cert-bund: CB-K18/0635
cert-bund: CB-K18/0550
cert-bund: CB-K18/0523
cert-bund: CB-K18/0487
cert-bund: CB-K17/0792
cert-bund: CB-K17/0727
dfn-cert: DFN-CERT-2019-2614
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2067
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1760
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1549
dfn-cert: DFN-CERT-2018-1494
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1279
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1190
dfn-cert: DFN-CERT-2018-1123
dfn-cert: DFN-CERT-2018-1121
dfn-cert: DFN-CERT-2018-1072
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0972
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0888
dfn-cert: DFN-CERT-2018-0887
dfn-cert: DFN-CERT-2018-0883
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0765
dfn-cert: DFN-CERT-2018-0755
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0560
dfn-cert: DFN-CERT-2018-0516
dfn-cert: DFN-CERT-2017-0820
dfn-cert: DFN-CERT-2017-0742
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3698-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3698-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.153.163
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

It was discovered that the nested KVM implementation in the Linux kernel in some situations did not properly prevent second level guests from reading and writing the hardware CR8 register. A local attacker in a guest could use this to cause a denial of service (system crash). (CVE-2017-12154)

Fan Wu, Haoran Qiu, and Shixiong Zhao discovered that the associative array implementation in the Linux kernel sometimes did not properly handle adding a new entry. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-12193)

It was discovered that a race condition existed in the ALSA subsystem of the Linux kernel when creating and deleting a port via ioctl(). A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-15265)

It was discovered that a null pointer dereference vulnerability existed in the DCCP protocol implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2018-1130)

Julian Stecklina and Thomas Prescher discovered that FPU register states (such as MMX, SSE, and AVX registers) which are lazily restored are potentially vulnerable to a side channel attack. A local attacker could use this to expose sensitive information. (CVE-2018-3665)

Wang Qize discovered that an information disclosure vulnerability existed in the SMBus driver for ACPI Embedded Controllers in the Linux kernel. A local attacker could use this to expose sensitive information (kernel pointer addresses). (CVE-2018-5750)

It was discovered that the SCTP Protocol implementation in the Linux kernel did not properly validate userspace provided payload lengths in some situations. A local attacker could use this to cause a denial of service (system crash). (CVE-2018-5803)

It was discovered that an integer overflow error existed in the futex implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2018-6927)

It was discovered that an information leak vulnerability existed in the floppy driver in the Linux kernel. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2018-7755)

It was discovered that a memory leak existed in the SAS driver subsystem of the Linux kernel. A local attacker could use this to cause a denial of service (memory exhaustion). (CVE-2018-7757)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3698-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3698.1
Version used: `2023-06-23T04:09:37Z`

References

```
url: https://ubuntu.com/security/notices/USN-3698-1
cve: CVE-2017-12154
cve: CVE-2017-12193
cve: CVE-2017-15265
cve: CVE-2018-1130
cve: CVE-2018-3665
cve: CVE-2018-5750
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-5803
cve: CVE-2018-6927
cve: CVE-2018-7755
cve: CVE-2018-7757
advisory_id: USN-3698-1
cert-bund: WID-SEC-2022-0532
cert-bund: WID-SEC-2022-0309
cert-bund: CB-K19/0774
cert-bund: CB-K19/0271
cert-bund: CB-K18/0765
cert-bund: CB-K18/0757
cert-bund: CB-K18/0730
cert-bund: CB-K18/0722
cert-bund: CB-K18/0664
cert-bund: CB-K18/0635
cert-bund: CB-K18/0550
cert-bund: CB-K18/0440
cert-bund: CB-K18/0346
cert-bund: CB-K18/0272
cert-bund: CB-K18/0244
cert-bund: CB-K18/0222
cert-bund: CB-K18/0165
cert-bund: CB-K18/0160
cert-bund: CB-K18/0049
cert-bund: CB-K17/2213
cert-bund: CB-K17/2193
cert-bund: CB-K17/2169
cert-bund: CB-K17/2146
cert-bund: CB-K17/2144
cert-bund: CB-K17/2129
cert-bund: CB-K17/2098
cert-bund: CB-K17/2081
cert-bund: CB-K17/2008
cert-bund: CB-K17/1998
cert-bund: CB-K17/1908
cert-bund: CB-K17/1885
cert-bund: CB-K17/1867
cert-bund: CB-K17/1850
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1837
cert-bund: CB-K17/1813
cert-bund: CB-K17/1812
cert-bund: CB-K17/1772
cert-bund: CB-K17/1742
cert-bund: CB-K17/1607
cert-bund: CB-K17/1568
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-0376
dfn-cert: DFN-CERT-2022-1375
dfn-cert: DFN-CERT-2022-1341
dfn-cert: DFN-CERT-2022-1092
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1673
dfn-cert: DFN-CERT-2019-1631
dfn-cert: DFN-CERT-2019-1554
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0607
dfn-cert: DFN-CERT-2019-0115
dfn-cert: DFN-CERT-2019-0101
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0025
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2550
dfn-cert: DFN-CERT-2018-2548
dfn-cert: DFN-CERT-2018-2526
dfn-cert: DFN-CERT-2018-2507
dfn-cert: DFN-CERT-2018-2498
dfn-cert: DFN-CERT-2018-2497
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2359
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2288
dfn-cert: DFN-CERT-2018-2287
dfn-cert: DFN-CERT-2018-2280
dfn-cert: DFN-CERT-2018-2262
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2129
dfn-cert: DFN-CERT-2018-2060
dfn-cert: DFN-CERT-2018-2029
dfn-cert: DFN-CERT-2018-2023
dfn-cert: DFN-CERT-2018-1990
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1722
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1569
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1468
dfn-cert: DFN-CERT-2018-1452
dfn-cert: DFN-CERT-2018-1446
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1404
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1355
dfn-cert: DFN-CERT-2018-1352
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1337
dfn-cert: DFN-CERT-2018-1332
dfn-cert: DFN-CERT-2018-1293
dfn-cert: DFN-CERT-2018-1292
dfn-cert: DFN-CERT-2018-1290
dfn-cert: DFN-CERT-2018-1289
dfn-cert: DFN-CERT-2018-1288
dfn-cert: DFN-CERT-2018-1279
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1260
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1206
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1190
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1170
dfn-cert: DFN-CERT-2018-1150
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0972
dfn-cert: DFN-CERT-2018-0947
dfn-cert: DFN-CERT-2018-0914
dfn-cert: DFN-CERT-2018-0882
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0780
dfn-cert: DFN-CERT-2018-0737
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0592
dfn-cert: DFN-CERT-2018-0470
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0288
dfn-cert: DFN-CERT-2018-0267
dfn-cert: DFN-CERT-2018-0237
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0178
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2017-2314
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2246
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2223
dfn-cert: DFN-CERT-2017-2192
dfn-cert: DFN-CERT-2017-2176
dfn-cert: DFN-CERT-2017-2099
dfn-cert: DFN-CERT-2017-2092
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1967
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1932
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1921
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1892
dfn-cert: DFN-CERT-2017-1847
dfn-cert: DFN-CERT-2017-1820
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1632
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3510-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3510-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.137.146
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Mohamed Ghannam discovered that a use-after-free vulnerability existed in the Netlink subsystem (XFRM) in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-16939)

. . . continues on next page . . .

... continued from previous page ...

It was discovered that the Linux kernel did not properly handle copy-on- write of transparent huge pages. A local attacker could use this to cause a denial of service (application crashes) or possibly gain administrative privileges. (CVE-2017-1000405)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3510-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3510.1
Version used: `2023-01-23T04:10:55Z`

References

```
url: https://ubuntu.com/security/notices/USN-3510-1
cve: CVE-2017-1000405
cve: CVE-2017-16939
advisory_id: USN-3510-1
cert-bund: WID-SEC-2023-0527
cert-bund: CB-K19/0774
cert-bund: CB-K18/0222
cert-bund: CB-K18/0183
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0017
cert-bund: CB-K17/2193
cert-bund: CB-K17/2182
cert-bund: CB-K17/2169
cert-bund: CB-K17/2129
cert-bund: CB-K17/2125
cert-bund: CB-K17/2116
cert-bund: CB-K17/2099
cert-bund: CB-K17/2098
dfn-cert: DFN-CERT-2020-2562
dfn-cert: DFN-CERT-2020-2555
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-1151
dfn-cert: DFN-CERT-2018-1147
dfn-cert: DFN-CERT-2018-0888
dfn-cert: DFN-CERT-2018-0887
dfn-cert: DFN-CERT-2018-0237
dfn-cert: DFN-CERT-2018-0198
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0058
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2017-2293
dfn-cert: DFN-CERT-2017-2281
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2224
dfn-cert: DFN-CERT-2017-2223
dfn-cert: DFN-CERT-2017-2212
dfn-cert: DFN-CERT-2017-2192
dfn-cert: DFN-CERT-2017-2184
```

High (CVSS: 7.8)
NVT: Ubuntu: Security Advisory (USN-3470-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3470-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.135.144
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Qian Zhang discovered a heap-based buffer overflow in the tipc_msg_build() function in the Linux kernel. A local attacker could use to cause a denial of service (system crash) or possibly execute arbitrary code with administrative privileges. (CVE-2016-8632)
Dmitry Vyukov discovered that a race condition existed in the timerfd subsystem of the Linux kernel when handling might_cancel queuing. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-10661)
It was discovered that the Flash-Friendly File System (f2fs) implementation in the Linux kernel did not properly validate superblock metadata. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-10662, CVE-2017-10663)
Anthony Perard discovered that the Xen virtual block driver did not properly initialize some data structures before passing them to user space. A local attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs. (CVE-2017-10911)
It was discovered that a use-after-free vulnerability existed in the POSIX message queue 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-2017-11176)

. . . continues on next page . . .

. . . continued from previous page . . .

Dave Chinner discovered that the XFS filesystem did not enforce that the realtime inode flag was settable only on filesystems on a realtime device. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-14340)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3470-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3470.1
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-3470-1
cve: CVE-2016-8632
cve: CVE-2017-10661
cve: CVE-2017-10662
cve: CVE-2017-10663
cve: CVE-2017-10911
cve: CVE-2017-11176
cve: CVE-2017-14340
advisory_id: USN-3470-1
cert-bund: CB-K18/0184
cert-bund: CB-K18/0166
cert-bund: CB-K18/0049
cert-bund: CB-K18/0022
cert-bund: CB-K17/2182
cert-bund: CB-K17/2169
cert-bund: CB-K17/2144
cert-bund: CB-K17/2141
cert-bund: CB-K17/2124
cert-bund: CB-K17/1897
cert-bund: CB-K17/1890
cert-bund: CB-K17/1874
cert-bund: CB-K17/1869
cert-bund: CB-K17/1868
cert-bund: CB-K17/1867
cert-bund: CB-K17/1850
cert-bund: CB-K17/1849
cert-bund: CB-K17/1804
cert-bund: CB-K17/1776
cert-bund: CB-K17/1696
cert-bund: CB-K17/1607
cert-bund: CB-K17/1584
cert-bund: CB-K17/1578
cert-bund: CB-K17/1552
cert-bund: CB-K17/1530
cert-bund: CB-K17/1484
cert-bund: CB-K17/1449
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1408
cert-bund: CB-K17/1329
cert-bund: CB-K17/1325
cert-bund: CB-K17/1253
cert-bund: CB-K17/1236
cert-bund: CB-K17/1195
cert-bund: CB-K17/1115
cert-bund: CB-K17/0941
cert-bund: CB-K17/0697
cert-bund: CB-K17/0552
cert-bund: CB-K17/0297
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0202
cert-bund: CB-K17/0168
cert-bund: CB-K17/0122
cert-bund: CB-K16/1900
cert-bund: CB-K16/1890
dfn-cert: DFN-CERT-2020-0023
dfn-cert: DFN-CERT-2019-2552
dfn-cert: DFN-CERT-2018-2550
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-1819
dfn-cert: DFN-CERT-2018-1723
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0182
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2017-2281
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2241
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-2225
dfn-cert: DFN-CERT-2017-1984
dfn-cert: DFN-CERT-2017-1970
dfn-cert: DFN-CERT-2017-1957
dfn-cert: DFN-CERT-2017-1951
dfn-cert: DFN-CERT-2017-1950
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1932
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1887
dfn-cert: DFN-CERT-2017-1852
dfn-cert: DFN-CERT-2017-1778
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1646
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-1621
dfn-cert: DFN-CERT-2017-1596
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1513
dfn-cert: DFN-CERT-2017-1472
dfn-cert: DFN-CERT-2017-1378
dfn-cert: DFN-CERT-2017-1376
dfn-cert: DFN-CERT-2017-1299
dfn-cert: DFN-CERT-2017-1278
dfn-cert: DFN-CERT-2017-1234
dfn-cert: DFN-CERT-2017-1155
dfn-cert: DFN-CERT-2017-0972
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0207
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2017-0124
dfn-cert: DFN-CERT-2016-2011
dfn-cert: DFN-CERT-2016-2004
```

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.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm11
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm11
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm13
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm13
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2022-11-14T04:23:33Z`

References

```
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-4256-1)

Summary
The remote host is missing an update for the 'cyrus-sasl2' package(s) announced via the USN-4256-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsasl2-2
Installed version:    libsasl2-2-2.1.25.dfsg1-17build1
Fixed version:      >=libsasl2-2-2.1.25.dfsg1-17ubuntu0.1~esm1
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'cyrus-sasl2' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that Cyrus SASL incorrectly handled certain LDAP packets. An attacker could possibly use this issue to 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-4256-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4256.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4256-1
cve: CVE-2019-19906
advisory_id: USN-4256-1
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: CB-K20/0730
cert-bund: CB-K20/0722
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2020-1556
dfn-cert: DFN-CERT-2020-1555
dfn-cert: DFN-CERT-2020-0031
dfn-cert: DFN-CERT-2019-2692
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4466-2)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-4466-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm5
Vulnerable package:   libcurl3-gnutls
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:       >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm5
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4466-1 fixed a vulnerability in curl. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Marc Aldorasi discovered that curl incorrectly handled the libcurl CURLOPT_CONNECT_ONLY option. This could result in data being sent to the wrong destination, possibly exposing sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4466-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4466.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4466-2
cve: CVE-2020-8231
advisory_id: USN-4466-2
cert-bund: WID-SEC-2023-1635
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-1061
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2020-2695
dfn-cert: DFN-CERT-2020-1818
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4665-2)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-4665-2 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm6
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm6
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm6
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4665-1 fixed several vulnerabilities in curl. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Varnavas Papaioannou discovered that curl incorrectly handled FTP PASV responses. An attacker could possibly use this issue to trick curl into connecting to an arbitrary IP address and be used to perform port scanner and other information gathering. (CVE-2020-8284)
It was discovered that curl incorrectly handled FTP wildcard matchins. A remote attacker could possibly use this issue to cause curl to consume resources and crash, resulting in a denial of service. (CVE-2020-8285)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4665-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4665.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4665-2
cve: CVE-2020-8284
cve: CVE-2020-8285
advisory_id: USN-4665-2
cert-bund: WID-SEC-2023-1350
cert-bund: CB-K22/0061
cert-bund: CB-K21/0446
cert-bund: CB-K20/1210
dfn-cert: DFN-CERT-2022-0121
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-0868
dfn-cert: DFN-CERT-2021-0867
dfn-cert: DFN-CERT-2021-0866
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2021-0042
dfn-cert: DFN-CERT-2020-2695
dfn-cert: DFN-CERT-2020-2683
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5079-2)

Summary
The remote host is missing an update for the ’curl’ package(s) announced via the USN-5079-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm8
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm8
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm8
```

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

Affected Software/OS
’curl’ package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5079-1 fixed several vulnerabilities in curl. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-5079-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5079.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5079-2
cve: CVE-2021-22946
cve: CVE-2021-22947
advisory_id: USN-5079-2
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
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-2021-1931
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5079-4)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5079-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm9
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm9
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm9
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5079-2 fixed vulnerabilities in curl. One of the fixes introduced a regression. This update fixes the problem.
Original advisory details:
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-5079-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5079.4
Version used: `2022-09-16T08:45:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5079-4
url: https://launchpad.net/bugs/1944120
cve: CVE-2021-22946
cve: CVE-2021-22947
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-5079-4
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1461
cert-bund: WID-SEC-2022-1335
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-2021-1931
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5499-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5499-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm11
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm11
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm11
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
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 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-5499-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5499.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5499-1
cve: CVE-2022-27781
cve: CVE-2022-32208
advisory_id: USN-5499-1
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-2022-1846
cert-bund: WID-SEC-2022-0479
cert-bund: WID-SEC-2022-0277
cert-bund: CB-K22/0570
dfn-cert: DFN-CERT-2023-0100
dfn-cert: DFN-CERT-2022-2799
dfn-cert: DFN-CERT-2022-2364
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1426
dfn-cert: DFN-CERT-2022-1140
dfn-cert: DFN-CERT-2022-1049
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4635-1)

Summary
The remote host is missing an update for the 'krb5' package(s) announced via the USN-4635-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   krb5-locales
Installed version:    krb5-locales-1.12+dfsg-2ubuntu5.4
Fixed version:      >=krb5-locales-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   krb5-multidev
Installed version:    krb5-multidev-1.12+dfsg-2ubuntu5.4
Fixed version:      >=krb5-multidev-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libgssapi-krb5-2
Installed version:    libgssapi-krb5-2-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libgssapi-krb5-2-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libgssrpc4
Installed version:    libgssrpc4-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libgssrpc4-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libk5crypto3
Installed version:    libk5crypto3-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libk5crypto3-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libkadm5clnt-mit9
Installed version:    libkadm5clnt-mit9-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkadm5clnt-mit9-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libkadm5srv-mit9
Installed version:    libkadm5srv-mit9-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkadm5srv-mit9-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libkdb5-7
Installed version:    libkdb5-7-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkdb5-7-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libkrb5-3
Installed version:    libkrb5-3-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkrb5-3-1.12+dfsg-2ubuntu5.4+esm2
Vulnerable package:   libkrb5support0
Installed version:    libkrb5support0-1.12+dfsg-2ubuntu5.4
Fixed version:      >=libkrb5support0-1.12+dfsg-2ubuntu5.4+esm2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'krb5' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10.

Vulnerability Insight
Demi Obenour discovered that Kerberos incorrectly handled certain ASN.1. 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-4635-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4635.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4635-1
cve: CVE-2020-28196
advisory_id: USN-4635-1
cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1481
cert-bund: WID-SEC-2022-0602
cert-bund: CB-K21/0421
cert-bund: CB-K20/1089
dfn-cert: DFN-CERT-2022-2323
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1209
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2020-2437
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4169-1)

Summary
The remote host is missing an update for the 'libarchive' package(s) announced via the USN-4169-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libarchive13
Installed version:    libarchive13-3.1.2-7ubuntu2.8
Fixed version:      >=libarchive13-3.1.2-7ubuntu2.8+esm1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'libarchive' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04.

Vulnerability Insight
It was discovered that libarchive incorrectly handled certain archive files. An attacker could possibly execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4169-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4169.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4169-1
cve: CVE-2019-18408
advisory_id: USN-4169-1
cert-bund: CB-K20/1049
cert-bund: CB-K19/0988
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2528
dfn-cert: DFN-CERT-2019-2527
dfn-cert: DFN-CERT-2019-2230
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4358-1)

Summary
The remote host is missing an update for the 'libexif' package(s) announced via the USN-4358-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexif12
Installed version:    libexif12-0.6.21-1ubuntu1
Fixed version:      >=libexif12-0.6.21-1ubuntu1+esm2
```

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

Affected Software/OS
'libexif' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

It was discovered that libexif incorrectly handled certain tags. An attacker could possibly use this issue to cause a denial of service. (CVE-2018-20030)
It was discovered that libexif incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash. (CVE-2020-12767)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4358-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4358.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4358-1
cve: CVE-2018-20030
cve: CVE-2020-12767
advisory_id: USN-4358-1
cert-bund: CB-K20/1030
cert-bund: CB-K20/0465
cert-bund: CB-K18/1182
dfn-cert: DFN-CERT-2020-2400
dfn-cert: DFN-CERT-2020-2135
dfn-cert: DFN-CERT-2020-1289
dfn-cert: DFN-CERT-2020-1190
dfn-cert: DFN-CERT-2020-1174
dfn-cert: DFN-CERT-2020-1132
dfn-cert: DFN-CERT-2020-1050
dfn-cert: DFN-CERT-2020-1034
dfn-cert: DFN-CERT-2020-0393
dfn-cert: DFN-CERT-2019-0300
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4040-2)

Summary

The remote host is missing an update for the 'expat' package(s) announced via the USN-4040-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.1.0-4ubuntu1.4
Fixed version:      >=libexpat1-2.1.0-4ubuntu1.4+esm1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'expat' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4040-1 fixed a vulnerability in expat. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Expat incorrectly handled certain XML 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-4040-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4040.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4040-2
cve: CVE-2018-20843
advisory_id: USN-4040-2
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K20/1030
cert-bund: CB-K19/0546
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0572
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2118
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2019-2169
dfn-cert: DFN-CERT-2019-1961
dfn-cert: DFN-CERT-2019-1298
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4132-2)

Summary
The remote host is missing an update for the 'expat' package(s) announced via the USN-4132-2 advisory.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   libexpat1
Installed version:    libexpat1-2.1.0-4ubuntu1.4
Fixed version:       >=libexpat1-2.1.0-4ubuntu1.4+esm2
```

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

Affected Software/OS
'expat' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4132-1 fixed a vulnerability in Expat. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Expat incorrectly handled certain XML 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-4132-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4132.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4132-2
cve: CVE-2019-15903
advisory_id: USN-4132-2
cert-bund: CB-K20/1030
cert-bund: CB-K19/1068
cert-bund: CB-K19/1065
cert-bund: CB-K19/1057
cert-bund: CB-K19/0937
cert-bund: CB-K19/0935
cert-bund: CB-K19/0934
cert-bund: CB-K19/0798
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0572
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2118
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0231
dfn-cert: DFN-CERT-2020-0111
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-2628
dfn-cert: DFN-CERT-2019-2627
dfn-cert: DFN-CERT-2019-2621
dfn-cert: DFN-CERT-2019-2618
dfn-cert: DFN-CERT-2019-2337
dfn-cert: DFN-CERT-2019-2220
dfn-cert: DFN-CERT-2019-2209
dfn-cert: DFN-CERT-2019-2205
dfn-cert: DFN-CERT-2019-1922
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4316-2)

Summary
The remote host is missing an update for the 'libgd2' package(s) announced via the USN-4316-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libgd3
Installed version:    libgd3-2.1.0-3ubuntu0.11
Fixed version:      >=libgd3-2.1.0-3ubuntu0.11+esm1
```

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

Affected Software/OS
'libgd2' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4316-1 fixed a vulnerability in GD Graphics Library. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that GD Graphics Library incorrectly handled cloning an image. An attacker could possibly use this issue to cause GD Graphics Library to crash, resulting in a denial of service. (CVE-2018-14553)
It was discovered that GD Graphics Library incorrectly handled loading images from X bitmap format files. An attacker could possibly use this issue to cause GD Graphics Library to crash, resulting in a denial of service, or to disclose contents of the stack that has been left there by previous code. (CVE-2019-11038)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4316-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4316.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4316-2
cve: CVE-2018-14553
cve: CVE-2019-11038
advisory_id: USN-4316-2
dfn-cert: DFN-CERT-2021-1930
dfn-cert: DFN-CERT-2020-2398
dfn-cert: DFN-CERT-2020-0484
dfn-cert: DFN-CERT-2020-0479
dfn-cert: DFN-CERT-2020-0462
dfn-cert: DFN-CERT-2020-0336
dfn-cert: DFN-CERT-2019-2283
dfn-cert: DFN-CERT-2019-1978
dfn-cert: DFN-CERT-2019-1796
dfn-cert: DFN-CERT-2019-1737
dfn-cert: DFN-CERT-2019-1174
dfn-cert: DFN-CERT-2019-1079
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4049-2)

Summary
The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-4049-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.40.2-0ubuntu1.1
Fixed version:      >=libglib2.0-0-2.40.2-0ubuntu1.1+esm2
```

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

Affected Software/OS
'glib2.0' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4049-1 fixed a vulnerability in GLib. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that GLib created directories and files without properly restricting permissions. An attacker could possibly use this issue to access 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-4049-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4049.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4049-2
cve: CVE-2019-13012
advisory_id: USN-4049-2
cert-bund: WID-SEC-2023-1155
cert-bund: CB-K19/0551
dfn-cert: DFN-CERT-2022-0024
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1081
dfn-cert: DFN-CERT-2019-1572
dfn-cert: DFN-CERT-2019-1367
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5672-2)

Summary

The remote host is missing an update for the 'gmp' package(s) announced via the USN-5672-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libgmp-dev
Installed version:    libgmp-dev-2:5.1.3+dfsg-1ubuntu1
Fixed version:      >=libgmp-dev-2:5.1.3+dfsg-1ubuntu1+esm1
Vulnerable package:   libgmp10
Installed version:    libgmp10-2:5.1.3+dfsg-1ubuntu1
Fixed version:      >=libgmp10-2:5.1.3+dfsg-1ubuntu1+esm1
Vulnerable package:   libgmpxx4ldbl
Installed version:    libgmpxx4ldbl-2:5.1.3+dfsg-1ubuntu1
Fixed version:      >=libgmpxx4ldbl-2:5.1.3+dfsg-1ubuntu1+esm1
```

Solution:

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

Affected Software/OS

'gmp' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

USN-5672-1 fixed a vulnerability in GMP. This update provides the corresponsing update for Ubuntu 14.04 ESM.
Original advisory details:
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-5672-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5672.2
Version used: `2023-03-07T04:11:40Z`

References

```
url: https://ubuntu.com/security/notices/USN-5672-2
cve: CVE-2021-43618
advisory_id: USN-5672-2
cert-bund: WID-SEC-2022-2024
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2021-2518
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm1
Vulnerable package:   libkrb5-26-heimdal
Installed version:    libkrb5-26-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libkrb5-26-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2023-04-05T13:55:58Z`

References

```
url: https://ubuntu.com/security/notices/USN-5675-1
cve: CVE-2018-16860
cve: CVE-2019-12098
cve: CVE-2021-3671
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.

Vulnerability Detection Result

```
Vulnerable package:   libgssapi3-heimdal
Installed version:    libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libgssapi3-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm4
```

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.

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: `2023-03-15T04:11:25Z`

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-4888-2)

Summary
The remote host is missing an update for the 'ldb' package(s) announced via the USN-4888-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libldb1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    libldb1-1:1.1.24-0ubuntu0.14.04.2
Fixed version:      >=libldb1-1:1.1.24-0ubuntu0.14.04.2+esm1
```

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

Affected Software/OS
'ldb' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4888-1 fixed several vulnerabilities in ldb. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain LDAP attributes. A remote attacker could possibly use this issue to cause the LDAP server to crash, resulting in a denial of service. (CVE-2021-20277)
Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain DN strings. A remote attacker could use this issue to cause the LDAP server to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-27840)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4888-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4888.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4888-2
cve: CVE-2020-27840
cve: CVE-2021-20277
advisory_id: USN-4888-2
cert-bund: CB-K21/0311
dfn-cert: DFN-CERT-2022-0242
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-0906
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0689
dfn-cert: DFN-CERT-2021-0674
dfn-cert: DFN-CERT-2021-0617
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5425-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'pcre3' package(s) announced via the USN-5425-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libpcre3
Installed version:    libpcre3-1:8.31-2ubuntu2.3
Fixed version:      >=libpcre3-1:8.31-2ubuntu2.3+esm1
```

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: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5425-1
cve: CVE-2019-20838
cve: CVE-2020-14155
advisory_id: USN-5425-1
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-2022-2305
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 7.5)
NVT: Ubuntu: Security Advisory (USN-4060-2)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4060-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm1
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4060-1 fixed several vulnerabilities in nss. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Henry Corrigan-Gibbs discovered that NSS incorrectly handled importing certain curve25519 private keys. An attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly obtain sensitive information. (CVE-2019-11719)
Jonas Allmann discovered that NSS incorrectly handled certain p256-ECDH public keys. An attacker could possibly use this issue to cause NSS to crash, resulting in a denial of service. (CVE-2019-11729)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4060-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4060.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4060-2
cve: CVE-2019-11719
cve: CVE-2019-11729
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-4060-2
cert-bund: WID-SEC-2023-0459
cert-bund: CB-K20/1030
cert-bund: CB-K19/0605
cert-bund: CB-K19/0584
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2137
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2019-2609
dfn-cert: DFN-CERT-2019-2112
dfn-cert: DFN-CERT-2019-2061
dfn-cert: DFN-CERT-2019-1951
dfn-cert: DFN-CERT-2019-1561
dfn-cert: DFN-CERT-2019-1491
dfn-cert: DFN-CERT-2019-1444
dfn-cert: DFN-CERT-2019-1420
dfn-cert: DFN-CERT-2019-1382
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4215-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4215-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm3
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04.

Vulnerability Insight
It was discovered that NSS incorrectly handled certain certificates. 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-4215-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4215.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4215-1
cve: CVE-2019-17007
advisory_id: USN-4215-1
dfn-cert: DFN-CERT-2021-0573
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2019-2579
dfn-cert: DFN-CERT-2019-2534
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4677-2)

Summary
The remote host is missing an update for the 'p11-kit' package(s) announced via the USN-4677-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libp11-kit0
Installed version:    libp11-kit0-0.20.2-2ubuntu2
Fixed version:      >=libp11-kit0-0.20.2-2ubuntu2+esm1
```

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

Affected Software/OS
'p11-kit' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4677-1 fixed a vulnerability in p11-kit. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
David Cook discovered that p11-kit incorrectly handled certain memory operations. An attacker could use this issue to cause p11-kit 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-4677-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4677.2
Version used: `2022-09-13T14:14:11Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-4677-2
cve: CVE-2020-29361
advisory_id: USN-4677-2
cert-bund: WID-SEC-2022-0702
cert-bund: CB-K21/0555
dfn-cert: DFN-CERT-2022-0264
dfn-cert: DFN-CERT-2021-2667
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2020-2734
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5767-2)

Summary
The remote host is missing an update for the 'python2.7, python3.5' package(s) announced via the USN-5767-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libpython2.7
Installed version:    libpython2.7-2.7.6-8ubuntu0.5
Fixed version:      >=libpython2.7-2.7.6-8ubuntu0.6+esm13
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm13
```

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

Affected Software/OS
'python2.7, python3.5' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5767-1 fixed a vulnerability in Python. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5767-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5767.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-12-09T04:10:14Z

References

```
url: https://ubuntu.com/security/notices/USN-5767-2
cve: CVE-2022-45061
advisory_id: USN-5767-2
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-2022-2043
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-2023-0120
dfn-cert: DFN-CERT-2023-0028
dfn-cert: DFN-CERT-2022-2793
dfn-cert: DFN-CERT-2022-2698
dfn-cert: DFN-CERT-2022-2658
dfn-cert: DFN-CERT-2022-2583
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5716-2)

Summary

The remote host is missing an update for the 'sqlite3' package(s) announced via the USN-5716-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libsqlite3-0
Installed version:    libsqlite3-0-3.8.2-1ubuntu2.2
Fixed version:      >=libsqlite3-0-3.8.2-1ubuntu2.2+esm3
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'sqlite3' package(s) on Ubuntu 14.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-5716-1 fixed a vulnerability in SQLite. This update provides the corresponding update for Ubuntu 14.04 ESM.

Original advisory details:

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-5716-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2022.5716.2

Version used: `2022-11-22T04:11:06Z`

References

```
url: https://ubuntu.com/security/notices/USN-5716-2
cve: CVE-2022-35737
advisory_id: USN-5716-2
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-2023-1590
dfn-cert: DFN-CERT-2022-2472
dfn-cert: DFN-CERT-2022-2306
dfn-cert: DFN-CERT-2022-2079
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libssl-doc
Installed version:    libssl-doc-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl-doc-1.0.1f-1ubuntu2.27+esm7
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm7
Vulnerable package:   openssl
Installed version:    openssl-1.0.1f-1ubuntu2.27
Fixed version:      >=openssl-1.0.1f-1ubuntu2.27+esm7
```

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: `2023-04-26T04:09:34Z`

References
```
url: https://ubuntu.com/security/notices/USN-6039-1
cve: CVE-2022-3996
cve: CVE-2023-0464
cve: CVE-2023-0465
cve: CVE-2023-0466
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-6039-1
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-2023-1428
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-2023-0904
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-5328-2)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5328-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm5
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5328-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

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-5328-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5328.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5328-2
cve: CVE-2022-0778
advisory_id: USN-5328-2
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-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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
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-5845-2)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5845-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm6
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5845-1 fixed several vulnerabilities in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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 . . .

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)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5845-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5845.2
Version used: `2023-02-23T04:11:04Z`

References

```
url: https://ubuntu.com/security/notices/USN-5845-2
cve: CVE-2023-0215
cve: CVE-2023-0286
advisory_id: USN-5845-2
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-2023-1590
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-2023-0543
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-6188-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'openssl' package(s) announced via the USN-6188-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm9
Vulnerable package:   openssl
Installed version:    openssl-1.0.1f-1ubuntu2.27
Fixed version:      >=openssl-1.0.1f-1ubuntu2.27+esm9
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6188-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6188.1
Version used: `2023-06-23T04:09:37Z`

References

```
url: https://ubuntu.com/security/notices/USN-6188-1
cve: CVE-2023-2650
advisory_id: USN-6188-1
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1323
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
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5523-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'tiff' package(s) announced via the USN-5523-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm2
```

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

Affected Software/OS
'tiff' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that LibTIFF was not properly performing 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-5523-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5523.1
Version used: `2022-09-13T14:14:11Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-5523-1
cve: CVE-2020-19131
cve: CVE-2020-19144
cve: CVE-2022-0907
cve: CVE-2022-0908
cve: CVE-2022-0909
cve: CVE-2022-0924
cve: CVE-2022-22844
advisory_id: USN-5523-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-0730
cert-bund: WID-SEC-2022-0728
cert-bund: WID-SEC-2022-0723
cert-bund: WID-SEC-2022-0220
dfn-cert: DFN-CERT-2022-2592
dfn-cert: DFN-CERT-2022-2494
dfn-cert: DFN-CERT-2022-2089
dfn-cert: DFN-CERT-2022-1601
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1109
dfn-cert: DFN-CERT-2022-1061
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
dfn-cert: DFN-CERT-2021-2100
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm4
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

'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 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: `2022-09-21T04:42:37Z`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2592
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-4199-2)

Summary
The remote host is missing an update for the 'libvpx' package(s) announced via the USN-4199-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libvpx1
Installed version:    libvpx1-1.3.0-2
Fixed version:      >=libvpx1-1.3.0-2ubuntu0.1~esm1
```

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

Affected Software/OS
'libvpx' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4199-1 fixed several vulnerabilities in libvpx. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that libvpx did not properly handle certain malformed WebM media files. If an application using libvpx opened a specially crafted WebM 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-4199-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4199.2
Version used: `2022-09-13T14:14:11Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-4199-2
cve: CVE-2017-13194
cve: CVE-2019-9232
cve: CVE-2019-9433
advisory_id: USN-4199-2
cert-bund: CB-K20/1030
cert-bund: CB-K19/0757
cert-bund: CB-K18/0104
cert-bund: CB-K18/0080
cert-bund: CB-K18/0004
dfn-cert: DFN-CERT-2020-2402
dfn-cert: DFN-CERT-2020-2114
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-0052
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2530
dfn-cert: DFN-CERT-2019-2510
dfn-cert: DFN-CERT-2019-2481
dfn-cert: DFN-CERT-2018-0115
dfn-cert: DFN-CERT-2018-0095
dfn-cert: DFN-CERT-2018-0008
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5637-1)

Summary
The remote host is missing an update for the 'libvpx' package(s) announced via the USN-5637-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libvpx1
Installed version:    libvpx1-1.3.0-2
Fixed version:      >=libvpx1-1.3.0-2ubuntu0.1~esm2
```

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

Affected Software/OS
'libvpx' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that libvpx incorrectly handled certain WebM media files. A remote attacker could use this issue to crash an application using libvpx under certain conditions, resulting in 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-5637-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5637.1
Version used: `2022-09-27T04:38:05Z`

References

```
url: https://ubuntu.com/security/notices/USN-5637-1
cve: CVE-2020-0034
advisory_id: USN-5637-1
cert-bund: CB-K20/1030
cert-bund: CB-K20/0186
dfn-cert: DFN-CERT-2020-2114
dfn-cert: DFN-CERT-2020-0483
dfn-cert: DFN-CERT-2020-0429
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libwind0-heimdal
Installed version:    libwind0-heimdal-1.6~git20131207+dfsg-1ubuntu1.2
Fixed version:      >=libwind0-heimdal-1.6~git20131207+dfsg-1ubuntu1.2+esm2
```

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 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: `2022-12-08T04:10:21Z`

. . . continues on next page . . .

. . . continued from previous page . . .

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-6168-2)

Summary

The remote host is missing an update for the 'libx11' package(s) announced via the USN-6168-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libx11-6
Installed version:    libx11-6-2:1.6.2-1ubuntu2.1
Fixed version:      >=libx11-6-2:1.6.2-1ubuntu2.1+esm3
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'libx11' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight

USN-6168-1 fixed a vulnerability in libx11. This update provides the corresponding update for Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 ESM.

Original advisory details:

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-6168-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2023.6168.2

Version used: `2023-07-10T04:09:33Z`

References

```
url: https://ubuntu.com/security/notices/USN-6168-2
cve: CVE-2023-3138
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
advisory_id: USN-6168-2
cert-bund: WID-SEC-2023-1485
dfn-cert: DFN-CERT-2023-1391
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4274-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the USN-4274-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.1+dfsg1-3ubuntu4.13
Fixed version:      >=libxml2-2.9.1+dfsg1-3ubuntu4.13+esm1
```

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

Affected Software/OS
'libxml2' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-19956, CVE-2020-7595)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4274-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4274.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4274-1
cve: CVE-2019-19956
cve: CVE-2020-7595
advisory_id: USN-4274-1
cert-bund: WID-SEC-2023-1614
cert-bund: CB-K20/1030
cert-bund: CB-K20/0708
cert-bund: CB-K20/0077
cert-bund: CB-K20/0054
dfn-cert: DFN-CERT-2021-1102
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0715
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-1989
dfn-cert: DFN-CERT-2020-1974
dfn-cert: DFN-CERT-2020-1335
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0930
dfn-cert: DFN-CERT-2020-0753
dfn-cert: DFN-CERT-2020-0729
dfn-cert: DFN-CERT-2020-0628
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2020-0312
dfn-cert: DFN-CERT-2020-0287
dfn-cert: DFN-CERT-2019-2708
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.1+dfsg1-3ubuntu4.13
Fixed version:      >=libxml2-2.9.1+dfsg1-3ubuntu4.13+esm3
```

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)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2022.5422.1
Version used: 2022-09-13T14:14:11Z

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-2023-1614
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

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-4164-1)

Summary
The remote host is missing an update for the 'libxslt' package(s) announced via the USN-4164-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxslt1.1
Installed version:    libxslt1.1-1.1.28-2ubuntu0.2
Fixed version:      >=libxslt1.1-1.1.28-2ubuntu0.2+esm1
```

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

Affected Software/OS
'libxslt' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that Libxslt incorrectly handled certain documents. An attacker could possibly use this issue to access sensitive information. This issue not affected Ubuntu 19.10. (CVE-2019-13117, CVE-2019-13118)
It was discovered that Libxslt incorrectly handled certain documents. An attacker could possibly use this issue to execute arbitrary code. (CVE-2019-18197)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-4164-1)
OID:1.3.6.1.4.1.25623.1.1.12.2019.4164.1
Version used: 2022-09-13T14:14:11Z

References
url: https://ubuntu.com/security/notices/USN-4164-1
cve: CVE-2019-13117
cve: CVE-2019-13118

. . . continues on next page . . .

... continued from previous page ...

```
cve: CVE-2019-18197
advisory_id: USN-4164-1
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-0234
cert-bund: WID-SEC-2022-1639
cert-bund: CB-K20/1030
cert-bund: CB-K20/0319
cert-bund: CB-K20/0097
cert-bund: CB-K20/0039
cert-bund: CB-K19/0652
cert-bund: CB-K19/0649
cert-bund: CB-K19/0644
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2131
dfn-cert: DFN-CERT-2020-1107
dfn-cert: DFN-CERT-2020-0771
dfn-cert: DFN-CERT-2020-0517
dfn-cert: DFN-CERT-2020-0513
dfn-cert: DFN-CERT-2020-0245
dfn-cert: DFN-CERT-2020-0095
dfn-cert: DFN-CERT-2020-0062
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2229
dfn-cert: DFN-CERT-2019-2207
dfn-cert: DFN-CERT-2019-1951
dfn-cert: DFN-CERT-2019-1522
dfn-cert: DFN-CERT-2019-1521
dfn-cert: DFN-CERT-2019-1512
dfn-cert: DFN-CERT-2019-1511
dfn-cert: DFN-CERT-2019-1501
dfn-cert: DFN-CERT-2019-1474
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-3741-3)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3741-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.156.166
```

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 14.04.

Vulnerability Insight
USN-3741-1 introduced mitigations in the Linux kernel for Ubuntu 14.04 LTS to address L1 Terminal Fault (L1TF) vulnerabilities (CVE-2018-3620, CVE-2018-3646). Unfortunately, the update introduced regressions that caused kernel panics when booting in some environments as well as preventing Java applications from starting. This update fixes the problems.
We apologize for the inconvenience.
Original advisory details:
It was discovered that memory present in the L1 data cache of an Intel CPU core may be exposed to a malicious process that is executing on the CPU core. This vulnerability is also known as L1 Terminal Fault (L1TF). A local attacker in a guest virtual machine could use this to expose sensitive information (memory from other guests or the host OS). (CVE-2018-3646)
It was discovered that memory present in the L1 data cache of an Intel CPU core may be exposed to a malicious process that is executing on the CPU core. This vulnerability is also known as L1 Terminal Fault (L1TF). A local attacker could use this to expose sensitive information (memory from the kernel or other processes). (CVE-2018-3620)
Juha-Matti Tilli discovered that the TCP implementation in the Linux kernel performed algorithmically expensive operations in some situations when handling incoming packets. A remote attacker could use this to cause a denial of service. (CVE-2018-5390)
Juha-Matti Tilli discovered that the IP implementation in the Linux kernel performed algorithmically expensive operations in some situations when handling incoming packet fragments. A remote attacker could use this to cause a denial of service. (CVE-2018-5391)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3741-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3741.3
Version used: `2022-12-30T04:10:31Z`

References
```
url: https://ubuntu.com/security/notices/USN-3741-3
url: https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1787258
url: https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1787127
cve: CVE-2018-3620
cve: CVE-2018-3646
cve: CVE-2018-5390
cve: CVE-2018-5391
advisory_id: USN-3741-3
cert-bund: WID-SEC-2023-0508
cert-bund: CB-K19/0047
cert-bund: CB-K18/1050
cert-bund: CB-K18/0913
cert-bund: CB-K18/0867
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0858
cert-bund: CB-K18/0854
cert-bund: CB-K18/0840
dfn-cert: DFN-CERT-2019-2262
dfn-cert: DFN-CERT-2019-2109
dfn-cert: DFN-CERT-2019-1483
dfn-cert: DFN-CERT-2019-1473
dfn-cert: DFN-CERT-2019-1371
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0740
dfn-cert: DFN-CERT-2019-0562
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0453
dfn-cert: DFN-CERT-2019-0442
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0004
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2398
dfn-cert: DFN-CERT-2018-2366
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2335
dfn-cert: DFN-CERT-2018-2260
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2182
dfn-cert: DFN-CERT-2018-2118
dfn-cert: DFN-CERT-2018-2117
dfn-cert: DFN-CERT-2018-2099
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-2063
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1943
dfn-cert: DFN-CERT-2018-1941
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1911
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1863
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1731
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1730
dfn-cert: DFN-CERT-2018-1722
dfn-cert: DFN-CERT-2018-1699
dfn-cert: DFN-CERT-2018-1677
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1666
dfn-cert: DFN-CERT-2018-1665
dfn-cert: DFN-CERT-2018-1661
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1654
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1652
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1650
dfn-cert: DFN-CERT-2018-1637
dfn-cert: DFN-CERT-2018-1635
dfn-cert: DFN-CERT-2018-1634
dfn-cert: DFN-CERT-2018-1632
dfn-cert: DFN-CERT-2018-1631
dfn-cert: DFN-CERT-2018-1629
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1626
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1623
dfn-cert: DFN-CERT-2018-1622
dfn-cert: DFN-CERT-2018-1621
dfn-cert: DFN-CERT-2018-1617
dfn-cert: DFN-CERT-2018-1615
dfn-cert: DFN-CERT-2018-1614
dfn-cert: DFN-CERT-2018-1605
dfn-cert: DFN-CERT-2018-1601
dfn-cert: DFN-CERT-2018-1553
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1547
dfn-cert: DFN-CERT-2018-1544
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-3742-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-3742-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
```

... continues on next page ...

. . . continued from previous page . . .

```
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:       >=linux-image-generic-3.13.0.155.165
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that memory present in the L1 data cache of an Intel CPU core may be exposed to a malicious process that is executing on the CPU core. This vulnerability is also known as L1 Terminal Fault (L1TF). A local attacker in a guest virtual machine could use this to expose sensitive information (memory from other guests or the host OS). (CVE-2018-3646)
It was discovered that memory present in the L1 data cache of an Intel CPU core may be exposed to a malicious process that is executing on the CPU core. This vulnerability is also known as L1 Terminal Fault (L1TF). A local attacker could use this to expose sensitive information (memory from the kernel or other processes). (CVE-2018-3620)
Andrey Konovalov discovered an out-of-bounds read in the POSIX timers subsystem in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or expose sensitive information. (CVE-2017-18344)
Juha-Matti Tilli discovered that the TCP implementation in the Linux kernel performed algorithmically expensive operations in some situations when handling incoming packets. A remote attacker could use this to cause a denial of service. (CVE-2018-5390)
Juha-Matti Tilli discovered that the IP implementation in the Linux kernel performed algorithmically expensive operations in some situations when handling incoming packet fragments. A remote attacker could use this to cause a denial of service. (CVE-2018-5391)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3742-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3742.1
Version used: 2022-12-30T04:10:31Z

References
```
url: https://ubuntu.com/security/notices/USN-3742-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/L1TF
cve: CVE-2017-18344
cve: CVE-2018-3620
cve: CVE-2018-3646
cve: CVE-2018-5390
cve: CVE-2018-5391
advisory_id: USN-3742-1
cert-bund: WID-SEC-2023-0508
cert-bund: CB-K19/0047
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/1050
cert-bund: CB-K18/0913
cert-bund: CB-K18/0867
cert-bund: CB-K18/0858
cert-bund: CB-K18/0854
cert-bund: CB-K18/0840
cert-bund: CB-K18/0835
dfn-cert: DFN-CERT-2019-2262
dfn-cert: DFN-CERT-2019-2109
dfn-cert: DFN-CERT-2019-1483
dfn-cert: DFN-CERT-2019-1473
dfn-cert: DFN-CERT-2019-1371
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-0740
dfn-cert: DFN-CERT-2019-0562
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0453
dfn-cert: DFN-CERT-2019-0442
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0004
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2398
dfn-cert: DFN-CERT-2018-2366
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2335
dfn-cert: DFN-CERT-2018-2260
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-2206
dfn-cert: DFN-CERT-2018-2182
dfn-cert: DFN-CERT-2018-2118
dfn-cert: DFN-CERT-2018-2117
dfn-cert: DFN-CERT-2018-2099
dfn-cert: DFN-CERT-2018-2072
dfn-cert: DFN-CERT-2018-2066
dfn-cert: DFN-CERT-2018-2063
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1943
dfn-cert: DFN-CERT-2018-1941
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1911
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1863
dfn-cert: DFN-CERT-2018-1829
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1822
dfn-cert: DFN-CERT-2018-1806
dfn-cert: DFN-CERT-2018-1782
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1731
dfn-cert: DFN-CERT-2018-1730
dfn-cert: DFN-CERT-2018-1722
dfn-cert: DFN-CERT-2018-1699
dfn-cert: DFN-CERT-2018-1677
dfn-cert: DFN-CERT-2018-1670
dfn-cert: DFN-CERT-2018-1666
dfn-cert: DFN-CERT-2018-1665
dfn-cert: DFN-CERT-2018-1661
dfn-cert: DFN-CERT-2018-1657
dfn-cert: DFN-CERT-2018-1656
dfn-cert: DFN-CERT-2018-1654
dfn-cert: DFN-CERT-2018-1653
dfn-cert: DFN-CERT-2018-1652
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1650
dfn-cert: DFN-CERT-2018-1637
dfn-cert: DFN-CERT-2018-1635
dfn-cert: DFN-CERT-2018-1634
dfn-cert: DFN-CERT-2018-1632
dfn-cert: DFN-CERT-2018-1631
dfn-cert: DFN-CERT-2018-1629
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1626
dfn-cert: DFN-CERT-2018-1625
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1623
dfn-cert: DFN-CERT-2018-1622
dfn-cert: DFN-CERT-2018-1621
dfn-cert: DFN-CERT-2018-1617
dfn-cert: DFN-CERT-2018-1615
dfn-cert: DFN-CERT-2018-1614
dfn-cert: DFN-CERT-2018-1605
dfn-cert: DFN-CERT-2018-1601
dfn-cert: DFN-CERT-2018-1553
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1547
dfn-cert: DFN-CERT-2018-1544
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4017-2)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux, linux-aws, linux-azure, linux-lts-trusty, linux-lts-xenial' package(s) announced via the USN-4017-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.171.182
```

Solution:

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

Affected Software/OS

'linux, linux-aws, linux-azure, linux-lts-trusty, linux-lts-xenial' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4017-1 fixed vulnerabilities in the Linux kernel for Ubuntu. This update provides the corresponding updates for the Linux kernel for Ubuntu 16.04 ESM and Ubuntu 14.04 ESM.
Jonathan Looney discovered that the TCP retransmission queue implementation in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. (CVE-2019-11478)
Jonathan Looney discovered that an integer overflow existed in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service (system crash). (CVE-2019-11477)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4017-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4017.2
Version used: `2023-01-19T04:10:57Z`

References

```
url: https://ubuntu.com/security/notices/USN-4017-2
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SACKPanic
cve: CVE-2019-11477
cve: CVE-2019-11478
advisory_id: USN-4017-2
cert-bund: WID-SEC-2023-0507
cert-bund: CB-K20/1028
cert-bund: CB-K20/0186
cert-bund: CB-K19/0516
cert-bund: CB-K19/0513
dfn-cert: DFN-CERT-2021-1503
dfn-cert: DFN-CERT-2021-0098
dfn-cert: DFN-CERT-2020-2304
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2252
dfn-cert: DFN-CERT-2020-0429
dfn-cert: DFN-CERT-2019-2532
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2262
dfn-cert: DFN-CERT-2019-2132
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1987
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1916
dfn-cert: DFN-CERT-2019-1612
dfn-cert: DFN-CERT-2019-1482
dfn-cert: DFN-CERT-2019-1443
dfn-cert: DFN-CERT-2019-1441
dfn-cert: DFN-CERT-2019-1416
dfn-cert: DFN-CERT-2019-1363
dfn-cert: DFN-CERT-2019-1265
dfn-cert: DFN-CERT-2019-1236
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1234
dfn-cert: DFN-CERT-2019-1233
dfn-cert: DFN-CERT-2019-1228
dfn-cert: DFN-CERT-2019-1226
dfn-cert: DFN-CERT-2019-1225
dfn-cert: DFN-CERT-2019-1224
dfn-cert: DFN-CERT-2019-1223
dfn-cert: DFN-CERT-2019-1222
dfn-cert: DFN-CERT-2019-1221
dfn-cert: DFN-CERT-2019-1218
dfn-cert: DFN-CERT-2019-1216
dfn-cert: DFN-CERT-2019-1215
dfn-cert: DFN-CERT-2019-1214
dfn-cert: DFN-CERT-2019-1212
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4151-2)

Summary
The remote host is missing an update for the 'python2.7, python3.4' package(s) announced via the USN-4151-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm3
Vulnerable package:   python2.7-minimal
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm3
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm4
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm4
```

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

Affected Software/OS
'python2.7, python3.4' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4151-1 fixed several vulnerabilities in Python. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Python incorrectly parsed certain email addresses. A remote attacker could possibly use this issue to trick Python applications into accepting email addresses that should be denied. (CVE-2019-16056)
It was discovered that the Python documentation XML-RPC server incorrectly handled certain fields. A remote attacker could use this issue to execute a cross-site scripting (XSS) attack. (CVE-2019-16935)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4151-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4151.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4151-2
cve: CVE-2019-16056
cve: CVE-2019-16935
advisory_id: USN-4151-2
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0710
cert-bund: CB-K20/0324
cert-bund: CB-K20/0109
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0790
dfn-cert: DFN-CERT-2020-2805
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2621
dfn-cert: DFN-CERT-2020-2386
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2278
dfn-cert: DFN-CERT-2020-2127
dfn-cert: DFN-CERT-2020-2117
dfn-cert: DFN-CERT-2020-2045
dfn-cert: DFN-CERT-2020-1839
dfn-cert: DFN-CERT-2020-1540
dfn-cert: DFN-CERT-2020-1537
dfn-cert: DFN-CERT-2020-0896
dfn-cert: DFN-CERT-2020-0550
dfn-cert: DFN-CERT-2020-0231
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2327
dfn-cert: DFN-CERT-2019-2252
dfn-cert: DFN-CERT-2019-2238
dfn-cert: DFN-CERT-2019-2210
dfn-cert: DFN-CERT-2019-2198
dfn-cert: DFN-CERT-2019-2113
dfn-cert: DFN-CERT-2019-2078
dfn-cert: DFN-CERT-2019-1883
dfn-cert: DFN-CERT-2019-1876
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4428-1)

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-4428-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm6
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm6
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm7
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm7
```

. . . continues on next page . . .

. . . continued from previous page . . .

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 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that Python documentation had a misleading information. A security issue could be possibly caused by wrong assumptions of this information. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-17514)
It was discovered that Python incorrectly handled certain TAR archives. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-20907)
It was discovered that incorrectly handled certain ZIP files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-9674)
It was discovered that Python incorrectly handled certain IP values. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. (CVE-2020-14422)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4428-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4428.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4428-1
cve: CVE-2019-17514
cve: CVE-2019-20907
cve: CVE-2019-9674
cve: CVE-2020-14422
advisory_id: USN-4428-1
cert-bund: WID-SEC-2023-1298
cert-bund: WID-SEC-2023-1220
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2770
dfn-cert: DFN-CERT-2020-2621
dfn-cert: DFN-CERT-2020-2588
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2550
dfn-cert: DFN-CERT-2020-2543
dfn-cert: DFN-CERT-2020-2393
dfn-cert: DFN-CERT-2020-2392
dfn-cert: DFN-CERT-2020-2386
dfn-cert: DFN-CERT-2020-2300
dfn-cert: DFN-CERT-2020-2278
dfn-cert: DFN-CERT-2020-2207
dfn-cert: DFN-CERT-2020-2045
dfn-cert: DFN-CERT-2020-2006
dfn-cert: DFN-CERT-2020-1839
dfn-cert: DFN-CERT-2020-1832
dfn-cert: DFN-CERT-2020-1613
dfn-cert: DFN-CERT-2020-1545
dfn-cert: DFN-CERT-2020-1540
dfn-cert: DFN-CERT-2020-1513
dfn-cert: DFN-CERT-2020-1427
dfn-cert: DFN-CERT-2020-1168
dfn-cert: DFN-CERT-2020-0694
dfn-cert: DFN-CERT-2020-0395
```

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.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm12
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm12
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2023-01-27T04:10:43Z`

References

```
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-2023-1517
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-5960-1)

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

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm14
```

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

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

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

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

References

```
url: https://ubuntu.com/security/notices/USN-5960-1
cve: CVE-2023-24329
advisory_id: USN-5960-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0513
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-6139-1)

. . . continues on next page . . .

. . . continued from previous page . . .

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.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm15
```

Solution:

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: `2023-06-06T04:09:27Z`

References

```
url: https://ubuntu.com/security/notices/USN-6139-1
cve: CVE-2023-24329
advisory_id: USN-6139-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0513
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-5083-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'python3.4, python3.5' package(s) announced via the USN-5083-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm11
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm11
```

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

Affected Software/OS
'python3.4, python3.5' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that Python incorrectly handled certain RFCs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 ESM. (CVE-2021-3733)
It was discovered that Python incorrectly handled certain server responses. An attacker could possibly use this issue to cause a denial of service. (CVE-2021-3737)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5083-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5083.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5083-1
cve: CVE-2021-3733
cve: CVE-2021-3737
advisory_id: USN-5083-1
cert-bund: WID-SEC-2023-1524
cert-bund: WID-SEC-2023-0141
cert-bund: WID-SEC-2022-0530
cert-bund: WID-SEC-2022-0432
cert-bund: WID-SEC-2022-0302
cert-bund: WID-SEC-2022-0144
cert-bund: WID-SEC-2022-0011
cert-bund: CB-K22/0129
dfn-cert: DFN-CERT-2023-1517
dfn-cert: DFN-CERT-2023-1423
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0121
dfn-cert: DFN-CERT-2022-1469
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-2021-2527
dfn-cert: DFN-CERT-2021-2353
dfn-cert: DFN-CERT-2021-2281
dfn-cert: DFN-CERT-2021-2207
dfn-cert: DFN-CERT-2021-1956
```

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.

Vulnerability Detection Result

```
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm12
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm12
```

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: `2022-09-13T14:14:11Z`

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-2023-1517
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-4986-2)

Summary
The remote host is missing an update for the 'rpcbind' package(s) announced via the USN-4986-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   rpcbind
Installed version:    rpcbind-0.2.1-2ubuntu2.2
Fixed version:      >=rpcbind-0.2.1-2ubuntu2.2+esm1
```

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

Affected Software/OS
'rpcbind' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-4986-1 fixed a vulnerability in rpcbind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind 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-4986-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4986.2
Version used: `2022-08-26T07:43:23Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-4986-2
cve: CVE-2017-8779
advisory_id: USN-4986-2
cert-bund: CB-K17/0776
dfn-cert: DFN-CERT-2018-1802
dfn-cert: DFN-CERT-2017-0786
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-3976-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-3976-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm1
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-3976-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Isaac Boukris and Andrew Bartlett discovered that Samba incorrectly checked S4U2Self packets. In certain environments, a remote attacker could possibly 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-3976-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3976.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3976-2
cve: CVE-2018-16860
advisory_id: USN-3976-2
cert-bund: WID-SEC-2022-1713
cert-bund: WID-SEC-2022-1712
cert-bund: CB-K19/0649
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0644
cert-bund: CB-K19/0396
dfn-cert: DFN-CERT-2022-2269
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-4341-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4341-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm6
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4341-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that Samba incorrectly handled certain LDAP queries. A remote attacker could possibly use this issue to cause Samba to consume resources, resulting in a denial of service. (CVE-2020-10704)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4341-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4341.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4341-2
cve: CVE-2020-10704
advisory_id: USN-4341-2
cert-bund: CB-K20/0626
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/0377
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2026
dfn-cert: DFN-CERT-2020-1578
dfn-cert: DFN-CERT-2020-0867
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4409-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4409-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm7
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10, Ubuntu 20.04.

Vulnerability Insight
Andrew Bartlett discovered that Samba incorrectly handled certain LDAP queries. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-10730)
Douglas Bagnall discovered that Samba incorrectly handled certain queries. A remote attacker could possibly use this issue to cause a denial of service. (CVE-2020-10745)
Andrei Popa discovered that Samba incorrectly handled certain LDAP queries. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 19.10 and Ubuntu 20.04 LTS. (CVE-2020-10760)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4409-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4409.1
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-4409-1`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-10730
cve: CVE-2020-10745
cve: CVE-2020-10760
advisory_id: USN-4409-1
cert-bund: CB-K20/0857
cert-bund: CB-K20/0657
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0674
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2026
dfn-cert: DFN-CERT-2020-1620
dfn-cert: DFN-CERT-2020-1614
dfn-cert: DFN-CERT-2020-1578
dfn-cert: DFN-CERT-2020-1417
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4454-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4454-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm8
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4454-1 fixed a vulnerability in Samba. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Martin von Wittich and Wilko Meyer discovered that Samba incorrectly handled certain empty UDP packets when being used as a AD DC NBT server. A remote attacker could possibly use this issue to cause Samba 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-4454-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4454.2

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4454-2
cve: CVE-2020-14303
advisory_id: USN-4454-2
cert-bund: CB-K20/0857
cert-bund: CB-K20/0657
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2026
dfn-cert: DFN-CERT-2020-1758
dfn-cert: DFN-CERT-2020-1578
dfn-cert: DFN-CERT-2020-1417
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-4692-1)

Summary
The remote host is missing an update for the 'tar' package(s) announced via the USN-4692-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   tar
Installed version:    tar-1.27.1-1ubuntu0.1
Fixed version:      >=tar-1.27.1-1ubuntu0.1+esm1
```

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

Affected Software/OS
'tar' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 20.10.

Vulnerability Insight
Chris Siebenmann discovered that tar incorrectly handled extracting files resized during extraction when invoked with the –sparse flag. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 12.04 ESM, Ubuntu 14.04 ESM, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-20482)
Daniel Axtens discovered that tar incorrectly handled certain malformed tar files. If a user or automated system were tricked into processing a specially crafted tar archive, a remote attacker could use this issue to cause tar to crash, resulting in a denial of service. (CVE-2019-9923)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4692-1)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2021.4692.1
Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4692-1
cve: CVE-2018-20482
cve: CVE-2019-9923
advisory_id: USN-4692-1
dfn-cert: DFN-CERT-2022-1014
dfn-cert: DFN-CERT-2019-0739
dfn-cert: DFN-CERT-2019-0563
dfn-cert: DFN-CERT-2019-0007
```

High (CVSS: 7.5)
NVT: Ubuntu: Security Advisory (USN-5355-2)

Summary

The remote host is missing an update for the 'zlib' package(s) announced via the USN-5355-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   zlib1g
Installed version:    zlib1g-1:1.2.8.dfsg-1ubuntu1.1
Fixed version:      >=zlib1g-1:1.2.8.dfsg-1ubuntu1.1+esm1
```

Solution:

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

Affected Software/OS

'zlib' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

USN-5355-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5355-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5355.2
Version used: 2022-09-13T14:14:11Z

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-5355-2
cve: CVE-2018-25032
advisory_id: USN-5355-2
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-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
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
```

. . . 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-2022-0768
dfn-cert: DFN-CERT-2022-0716
```

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-3335-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3335-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.121.131
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
It was discovered that the stack guard page for processes in the Linux kernel was not sufficiently large enough to prevent overlapping with the heap. An attacker could leverage this with another vulnerability to execute arbitrary code and gain administrative privileges

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3335-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3335.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3335-1
cve: CVE-2017-1000364
advisory_id: USN-3335-1
cert-bund: CB-K18/0184
cert-bund: CB-K17/2141
cert-bund: CB-K17/1719
cert-bund: CB-K17/1484
cert-bund: CB-K17/1429
cert-bund: CB-K17/1267
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/1261
cert-bund: CB-K17/1085
cert-bund: CB-K17/1042
cert-bund: CB-K17/1034
cert-bund: CB-K17/1029
cert-bund: CB-K17/1025
cert-bund: CB-K17/1020
cert-bund: CB-K17/1019
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2017-2232
dfn-cert: DFN-CERT-2017-1801
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1494
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-1308
dfn-cert: DFN-CERT-2017-1119
dfn-cert: DFN-CERT-2017-1080
dfn-cert: DFN-CERT-2017-1070
dfn-cert: DFN-CERT-2017-1062
dfn-cert: DFN-CERT-2017-1057
dfn-cert: DFN-CERT-2017-1056
dfn-cert: DFN-CERT-2017-1053
```

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-4969-2)

Summary
The remote host is missing an update for the 'isc-dhcp' package(s) announced via the USN-4969-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   isc-dhcp-client
Installed version:    isc-dhcp-client-4.2.4-7ubuntu12.12
Fixed version:      >=isc-dhcp-client-4.2.4-7ubuntu12.13+esm1
```

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

Affected Software/OS
'isc-dhcp' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-4969-1 fixed a vulnerability in DHCP. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

. . . continues on next page . . .

. . . continued from previous page . . .

Original advisory details:
Jon Franklin and Pawel Wieczorkiewicz discovered that DHCP incorrectly handled lease file parsing. A remote attacker could possibly use this issue to cause DHCP 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-4969-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4969.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4969-2
cve: CVE-2021-25217
advisory_id: USN-4969-2
cert-bund: WID-SEC-2023-1261
cert-bund: WID-SEC-2023-0063
cert-bund: CB-K21/0587
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1450
dfn-cert: DFN-CERT-2021-1356
dfn-cert: DFN-CERT-2021-1152
```

High (CVSS: 7.4)
NVT: Ubuntu: Security Advisory (USN-5051-2)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5051-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm3
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5051-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

. . . continues on next page . . .

... continued from previous page ...

Original advisory details:
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-5051-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5051.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5051-2
cve: CVE-2021-3712
advisory_id: USN-5051-2
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-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
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-K21/1087
cert-bund: CB-K21/0907
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0437
dfn-cert: DFN-CERT-2022-0122
dfn-cert: DFN-CERT-2022-0120
dfn-cert: DFN-CERT-2022-0118
dfn-cert: DFN-CERT-2022-0112
```

... continues on next page ...

. . . continued from previous page . . .

```
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-2021-2223
dfn-cert: DFN-CERT-2021-2188
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: 7.4)
NVT: Ubuntu: Security Advisory (USN-5051-4)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-5051-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm4
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-5051-2 introduced a regression in OpenSSL that affected only Ubuntu 14.04 ESM. This update fix the regression.
Original advisory details:
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-5051-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5051.4
Version used: `2022-09-16T08:45:11Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-5051-4
url: https://launchpad.net/bugs/1942357
cve: CVE-2021-3712
advisory_id: USN-5051-4
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-2022-0400
cert-bund: WID-SEC-2022-0393
cert-bund: WID-SEC-2022-0101
cert-bund: WID-SEC-2022-0094
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-K21/1087
cert-bund: CB-K21/0907
dfn-cert: DFN-CERT-2023-0469
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0437
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-2021-2223
dfn-cert: DFN-CERT-2021-2188
dfn-cert: DFN-CERT-2021-1996
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1871
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1799
```

High (CVSS: 7.3)
NVT: Ubuntu: Security Advisory (USN-4176-1)

Summary
The remote host is missing an update for the 'cpio' package(s) announced via the USN-4176-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   cpio
Installed version:    cpio-2.11+dfsg-1ubuntu1.2
Fixed version:      >=cpio-2.11+dfsg-1ubuntu1.2+esm1
```

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

Affected Software/OS
'cpio' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04, Ubuntu 19.10.

Vulnerability Insight
Thomas Habets discovered that GNU cpio incorrectly handled certain inputs. An attacker could possibly use this issue to privilege escalation.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4176-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4176.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4176-1
cve: CVE-2019-14866
advisory_id: USN-4176-1
cert-bund: WID-SEC-2023-1353
cert-bund: CB-K20/1030
dfn-cert: DFN-CERT-2023-1271
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2019-2293
```

High (CVSS: 7.2)
NVT: Ubuntu: Security Advisory (USN-4581-1)

Summary
The remote host is missing an update for the 'python2.7, python3.4, python3.5, python3.6' package(s) announced via the USN-4581-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm7
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm7
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm8
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm8
```

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

Affected Software/OS
'python2.7, python3.4, python3.5, python3.6' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
It was discovered that Python incorrectly handled certain character sequences. A remote attacker could possibly use this issue to perform CRLF injection.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4581-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4581.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4581-1
cve: CVE-2020-26116
advisory_id: USN-4581-1
cert-bund: WID-SEC-2022-0492
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2023-0082
dfn-cert: DFN-CERT-2022-1438
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1330
dfn-cert: DFN-CERT-2021-1080
dfn-cert: DFN-CERT-2021-1079
dfn-cert: DFN-CERT-2021-1071
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2621
dfn-cert: DFN-CERT-2020-2543
dfn-cert: DFN-CERT-2020-2300
dfn-cert: DFN-CERT-2020-2278
dfn-cert: DFN-CERT-2020-2207
dfn-cert: DFN-CERT-2020-1940
```

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-4392-1)

Summary
The remote host is missing an update for the 'linux, linux-lts-trusty' package(s) announced via the USN-4392-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.180.189
```

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

Affected Software/OS
'linux, linux-lts-trusty' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
It was discovered that the Marvell WiFi-Ex Driver in the Linux kernel did not properly validate status lengths in messages received from an access point, leading to a buffer overflow. A physically proximate attacker controlling an access point could use this to construct messages that could possibly result in arbitrary code execution. (CVE-2020-12654)
It was discovered that memory contents previously stored in microarchitectural special registers after RDRAND, RDSEED, and SGX EGETKEY read operations on Intel client and Xeon E3 processors may be briefly exposed to processes on the same or different processor cores. A local attacker could use this to expose sensitive information. (CVE-2020-0543)

. . . continues on next page . . .

. . . continued from previous page . . .

Piotr Krysiuk discovered that race conditions existed in the file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2020-12114)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4392-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4392.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4392-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SRBDS
cve: CVE-2020-0543
cve: CVE-2020-12114
cve: CVE-2020-12654
advisory_id: USN-4392-1
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1924
cert-bund: WID-SEC-2022-1849
cert-bund: WID-SEC-2022-1466
cert-bund: CB-K20/0873
cert-bund: CB-K20/0585
cert-bund: CB-K20/0562
cert-bund: CB-K20/0557
cert-bund: CB-K20/0420
cert-bund: CB-K20/0412
dfn-cert: DFN-CERT-2022-2448
dfn-cert: DFN-CERT-2022-2080
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-1993
dfn-cert: DFN-CERT-2021-1986
dfn-cert: DFN-CERT-2021-1689
dfn-cert: DFN-CERT-2021-1190
dfn-cert: DFN-CERT-2021-1084
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2021-0095
dfn-cert: DFN-CERT-2020-2253
dfn-cert: DFN-CERT-2020-2158
dfn-cert: DFN-CERT-2020-1983
dfn-cert: DFN-CERT-2020-1969
dfn-cert: DFN-CERT-2020-1929
dfn-cert: DFN-CERT-2020-1921
dfn-cert: DFN-CERT-2020-1739
dfn-cert: DFN-CERT-2020-1671
dfn-cert: DFN-CERT-2020-1669
dfn-cert: DFN-CERT-2020-1667
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-1663
dfn-cert: DFN-CERT-2020-1615
dfn-cert: DFN-CERT-2020-1598
dfn-cert: DFN-CERT-2020-1597
dfn-cert: DFN-CERT-2020-1503
dfn-cert: DFN-CERT-2020-1500
dfn-cert: DFN-CERT-2020-1495
dfn-cert: DFN-CERT-2020-1488
dfn-cert: DFN-CERT-2020-1477
dfn-cert: DFN-CERT-2020-1462
dfn-cert: DFN-CERT-2020-1364
dfn-cert: DFN-CERT-2020-1319
dfn-cert: DFN-CERT-2020-1291
dfn-cert: DFN-CERT-2020-1287
dfn-cert: DFN-CERT-2020-1277
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2020-1264
dfn-cert: DFN-CERT-2020-1258
dfn-cert: DFN-CERT-2020-1257
dfn-cert: DFN-CERT-2020-1256
dfn-cert: DFN-CERT-2020-1255
dfn-cert: DFN-CERT-2020-1254
dfn-cert: DFN-CERT-2020-1253
dfn-cert: DFN-CERT-2020-1252
dfn-cert: DFN-CERT-2020-1251
dfn-cert: DFN-CERT-2020-1250
dfn-cert: DFN-CERT-2020-1249
dfn-cert: DFN-CERT-2020-1248
dfn-cert: DFN-CERT-2020-1247
dfn-cert: DFN-CERT-2020-1246
dfn-cert: DFN-CERT-2020-1244
dfn-cert: DFN-CERT-2020-1243
dfn-cert: DFN-CERT-2020-1238
dfn-cert: DFN-CERT-2020-1232
dfn-cert: DFN-CERT-2020-1123
```

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-4015-2)

Summary
The remote host is missing an update for the 'dbus' package(s) announced via the USN-4015-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   dbus
Installed version:    dbus-1.6.18-0ubuntu4.4
Fixed version:      >=dbus-1.6.18-0ubuntu4.5+esm1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   libdbus-1-3
Installed version:    libdbus-1-3-1.6.18-0ubuntu4.4
Fixed version:      >=libdbus-1-3-1.6.18-0ubuntu4.5+esm1
```

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

Affected Software/OS
'dbus' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4015-1 fixed a vulnerability in DBus. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Joe Vennix discovered that DBus incorrectly handled DBUS_COOKIE_SHA1 authentication. A local attacker could possibly use this issue to bypass authentication and connect to DBus servers with elevated privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4015-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4015.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4015-2
cve: CVE-2019-12749
advisory_id: USN-4015-2
cert-bund: WID-SEC-2022-2007
cert-bund: CB-K20/1030
cert-bund: CB-K19/0510
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-1173
```

High (CVSS: 7.1)
NVT: Ubuntu: Security Advisory (USN-5056-1)

Summary
The remote host is missing an update for the 'apr' package(s) announced via the USN-5056-1 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libapr1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    libapr1-1.5.0-1
Fixed version:      >=libapr1-1.5.0-1ubuntu0.1~esm1
```

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

Affected Software/OS
'apr' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 21.04.

Vulnerability Insight
It was discovered that APR incorrectly handled certain inputs. 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-5056-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5056.1
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-5056-1
cve: CVE-2021-35940
advisory_id: USN-5056-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0064
cert-bund: WID-SEC-2022-0757
dfn-cert: DFN-CERT-2022-1610
dfn-cert: DFN-CERT-2022-0207
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-1832
```

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.

Vulnerability Detection Result
```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm1
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2022-09-13T14:14:11Z`

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-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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-2371
dfn-cert: DFN-CERT-2021-0702
```

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-3219-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3219-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.112.120
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Alexander Popov discovered that the N_HDLC line discipline 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 gain administrative privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3219-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3219.1
Version used: `2023-02-13T04:10:52Z`

References

```
url: https://ubuntu.com/security/notices/USN-3219-1
cve: CVE-2017-2636
advisory_id: USN-3219-1
cert-bund: CB-K17/1484
cert-bund: CB-K17/1323
cert-bund: CB-K17/1267
cert-bund: CB-K17/0838
cert-bund: CB-K17/0628
cert-bund: CB-K17/0605
cert-bund: CB-K17/0552
cert-bund: CB-K17/0546
cert-bund: CB-K17/0538
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0403
cert-bund: CB-K17/0401
cert-bund: CB-K17/0395
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1372
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0649
dfn-cert: DFN-CERT-2017-0626
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0554
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0408
dfn-cert: DFN-CERT-2017-0405
```

High (CVSS: 7.0)
NVT: Ubuntu: Security Advisory (USN-5484-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-5484-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.190.199
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

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)
It was discovered that a race condition existed in the network scheduling 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-2021-39713)
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-5484-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5484.1
Version used: `2022-10-21T04:34:40Z`

References

```
url: https://ubuntu.com/security/notices/USN-5484-1
cve: CVE-2021-39713
cve: CVE-2022-21123
cve: CVE-2022-21125
cve: CVE-2022-21166
cve: CVE-2022-21499
advisory_id: USN-5484-1
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
cert-bund: WID-SEC-2022-0112
cert-bund: WID-SEC-2022-0016
cert-bund: CB-K22/0651
cert-bund: CB-K22/0274
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-2022-2510
dfn-cert: DFN-CERT-2022-2502
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-2235
dfn-cert: DFN-CERT-2022-1847
dfn-cert: DFN-CERT-2022-1767
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-1604
dfn-cert: DFN-CERT-2022-1596
dfn-cert: DFN-CERT-2022-1586
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-2022-1510
dfn-cert: DFN-CERT-2022-1509
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-2022-1409
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-2022-1312
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-2022-1082
dfn-cert: DFN-CERT-2022-1071
dfn-cert: DFN-CERT-2022-0915
dfn-cert: DFN-CERT-2022-0864
dfn-cert: DFN-CERT-2022-0862
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2022-0860
dfn-cert: DFN-CERT-2022-0838
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0512
```

[return to 10.0.0.10]

2.1.4 High 631/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2022-08-01T10:11:45Z`

References

```
cve: CVE-2016-2183
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506
cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-0086
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[return to 10.0.0.10]

2.1.5 High 22/tcp

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2023-05-26T09:09:36Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2023-1944
```

[return to 10.0.0.10]

2.1.6 High 21/tcp

High (CVSS: 10.0)
NVT: ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Product detection result

```
cpe:/a:proftpd:proftpd:1.3.5
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)
```

Summary
ProFTPD is prone to an unauthenticated copying of files vulnerability.

Vulnerability Detection Result

```
The target was found to be vulnerable
```

Impact
Under some circumstances this could result in remote code execution

Solution:
Solution type: VendorFix
Ask the vendor for an update

Vulnerability Detection Method
Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO
Details: `ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO`
OID:1.3.6.1.4.1.25623.1.0.105254
Version used: `2022-12-02T10:11:16Z`

Product Detection Result
Product: `cpe:/a:proftpd:proftpd:1.3.5`
Method: `ProFTPD Server Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.900815)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2015-3306
url: http://bugs.proftpd.org/show_bug.cgi?id=4169
cert-bund: CB-K15/0791
cert-bund: CB-K15/0553
dfn-cert: DFN-CERT-2015-0839
dfn-cert: DFN-CERT-2015-0576
```

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting

Summary

It was possible to login into the remote FTP server using weak/known credentials.

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
```

Impact

This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Insight

The following devices are / software is known to be affected:

- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).

Details: `FTP Brute Force Logins Reporting`

OID:1.3.6.1.4.1.25623.1.0.108718

Version used: `2023-07-06T05:05:36Z`

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2018-19063
cve: CVE-2018-19064
```

[return to 10.0.0.10]

2.1.7 Medium general/tcp

Medium (CVSS: 6.8)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.

. . . continues on next page . . .

. . . continued from previous page . . .

- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.
- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108411
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 6.8)
NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight

Multiple flaws exist due to:

- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.
- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.
- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108411

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 6.8)

NVT: Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)

Product detection result

`cpe:/a:oracle:jdk:1.6.0:update_41`

. . . continues on next page . . .

... continued from previous page ...

```
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to bypass security restrictions, disclose sensitive information, manipulate certain data, conduct IP spoofing attacks or hijack a mutually authenticated session.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5 update 71 and prior, 6 update 81 and prior, 7 update 67 and prior, and 8 update 20 and prior on Linux

Vulnerability Insight
Multiple flaws exist due to:
- An unspecified error in share/classes/javax/crypto/CipherInputStream.java script related to streaming of input cipher streams.
- An error in share/classes/java/util/ResourceBundle.java script related to property processing and handling of names.
- An error in the 'LogRecord::readObject' function in classes/java/util/logging/LogRecord.java related to handling of resource bundles.
- An error related to the wrapping of datagram sockets in the DatagramSocket implementation.
- An error in share/classes/java/util/logging/Logger.java related to missing permission checks of logger resources.
- An error related to handling of server certificate changes during SSL/TLS renegotiation.
- An error within the 2D subcomponent of the client deployment.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Multiple Unspecified Vulnerabilities-01 Oct 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108411
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`

... continues on next page ...

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6558
cve: CVE-2014-6531
cve: CVE-2014-6502
cve: CVE-2014-6512
cve: CVE-2014-6511
cve: CVE-2014-6506
cve: CVE-2014-6457
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70533
url: http://www.securityfocus.com/bid/70538
url: http://www.securityfocus.com/bid/70544
url: http://www.securityfocus.com/bid/70548
url: http://www.securityfocus.com/bid/70556
url: http://www.securityfocus.com/bid/70567
url: http://www.securityfocus.com/bid/70572
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K15/0246
cert-bund: CB-K15/0237
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2015-0254
dfn-cert: DFN-CERT-2015-0245
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.8.3
Fixed version:     1.9.0
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/chef-13.8.5/distr
↪o/common/html/_static/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/2.4.0/rdoc/generator/template/dar
↪kfish/js/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/ruby-prof-0.17.0/
↪doc/js/jquery.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`

Method: `jQuery Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.150658)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/simplecov-html-0.
↪10.2/assets/javascripts/libraries/jquery-1.6.2.min.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rails-4.2.4/gui
↪des/assets/javascripts/jquery.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/lib/
↪rdoc/generator/template/darkfish/js/jquery.js
```

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/rails/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/sdoc/resources/js/jquery-1.3.2.min.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

`cve: CVE-2012-6708`

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.4
Fixed version:     1.9.0
Installation
path / port:       /usr/lib/ruby/1.9.1/rdoc/generator/template/darkfish/js/jquer
↪y.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /usr/lib/ruby/2.3.0/rdoc/generator/template/darkfish/js/jquer
↪y.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /usr/share/javascript/jquery/jquery.js
```

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`

Method: `jQuery Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.7.2
Fixed version:     1.9.0
Installation
path / port:       /usr/share/javascript/jquery/jquery.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References
```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result
`cpe:/a:jquery:jquery:1.6.2`

. . . continues on next page . . .

. . . continued from previous page . . .

```
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.4.4
Fixed version:     1.9.0
Installation
path / port:       /var/www/html/drupal/misc/jquery.js
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /var/www/html/phpmyadmin/js/jquery/jquery-1.6.2.js
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`

Method: `jQuery Detection Consolidation`

OID: 1.3.6.1.4.1.25623.1.0.150658)

... continues on next page ...

. . . continued from previous page . . .

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813683
Version used: `2022-07-26T10:10:42Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow attackers to cause some unspecified impacts.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108382
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
cve: CVE-2017-3509
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`
OID:1.3.6.1.4.1.25623.1.0.813683
Version used: `2022-07-26T10:10:42Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Successful exploitation will allow remote attackers to modify data, partially access data, cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.172 and earlier, 1.7.0.181 and earlier, 1.6.0.191 and earlier and 10.0 through 10.0.1 on Linux

Vulnerability Insight

Multiple flaws are due to multiple unspecified errors in components 'Libraries', 'JSSE' and 'Concurrency'.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates-02 (jul2018-4258247) - Linux`

OID:1.3.6.1.4.1.25623.1.0.813683

Version used: `2022-07-26T10:10:42Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2973
cve: CVE-2018-2940
cve: CVE-2018-2952
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
url: https://securitytracker.com/id/1041302
url: http://www.oracle.com/technetwork/java/javase/downloads/index.html
cert-bund: WID-SEC-2023-1308
cert-bund: CB-K19/0354
cert-bund: CB-K18/1076
cert-bund: CB-K18/0796
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-1902
dfn-cert: DFN-CERT-2018-1691
dfn-cert: DFN-CERT-2018-1675
dfn-cert: DFN-CERT-2018-1456
dfn-cert: DFN-CERT-2018-1405
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to cause some unspecified impacts.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108382
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2017-3509
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

Medium (CVSS: 5.9)
NVT: Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to cause some unspecified impacts.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.141 and earlier, 1.7.0.131 and earlier, 1.8.0.121 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to multiple unspecified errors in 'AWT', 'JCE', 'JAXP', 'Networking', 'Security' and 'Deployment' sub-components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (cpuapr2017-3236618) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108382
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2017-3514
cve: CVE-2017-3526
cve: CVE-2017-3509
cve: CVE-2017-3533
cve: CVE-2017-3544
cve: CVE-2017-3539
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
url: http://www.securityfocus.com/bid/97729
url: http://www.securityfocus.com/bid/97733
url: http://www.securityfocus.com/bid/97737
url: http://www.securityfocus.com/bid/97740
url: http://www.securityfocus.com/bid/97745
url: http://www.securityfocus.com/bid/97752
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
↪#AppendixJAVA
cert-bund: CB-K17/2168
cert-bund: CB-K17/1134
cert-bund: CB-K17/1133
cert-bund: CB-K17/0877
cert-bund: CB-K17/0784
cert-bund: CB-K17/0653
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2017-2268
dfn-cert: DFN-CERT-2017-1163
dfn-cert: DFN-CERT-2017-1162
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0806
dfn-cert: DFN-CERT-2017-0676
```

Medium (CVSS: 5.6)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

Vulnerability Insight

Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.

Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`

OID:1.3.6.1.4.1.25623.1.0.814405

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-06-29T10:11:11Z

Product Detection Result
Product: cpe:/a:oracle:jdk:1.6.0:update_41
Method: Multiple Java Products Version Detection (Linux)
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

Medium (CVSS: 5.6)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to multiple vulnerabilities.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

Vulnerability Insight

Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814405
Version used: `2022-06-29T10:11:11Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

Medium (CVSS: 5.6)
NVT: Oracle Java SE Security Updates-03 (cpuoct2018) - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     See reference
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to gain elevated privileges, cause partial denial of service conditions, partially modify and access data.

Solution:

Solution type: VendorFix

The vendor has released updates. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 through 1.6.0.201, 1.7.0 through 1.7.0.191, 1.8.0 through 1.8.0.181 and 11.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight
Multiple flaws are due to errors in components 'JNDI', 'Deployment (libpng)', 'Security', 'Networking' and 'JSSE'.

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates-03 (cpuoct2018) - Linux`
OID:1.3.6.1.4.1.25623.1.0.814405
Version used: `2022-06-29T10:11:11Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3149
cve: CVE-2018-13785
cve: CVE-2018-3136
cve: CVE-2018-3139
cve: CVE-2018-3180
cve: CVE-2018-14048
url: https://www.oracle.com/security-alerts/cpuoct2018.html#AppendixJAVA
advisory-id: cpuoct2018
cert-bund: CB-K19/1121
cert-bund: CB-K19/0175
cert-bund: CB-K19/0016
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2022-1175
dfn-cert: DFN-CERT-2020-0353
dfn-cert: DFN-CERT-2019-1110
dfn-cert: DFN-CERT-2019-0900
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0406
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2379
dfn-cert: DFN-CERT-2018-2107
dfn-cert: DFN-CERT-2018-1417
dfn-cert: DFN-CERT-2018-1361
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight

The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108368

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight

Multiple flaws are due to:

- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking component.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108384
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-3458
cve: CVE-2016-3485
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-2041
dfn-cert: DFN-CERT-2016-1449
dfn-cert: DFN-CERT-2016-1448
dfn-cert: DFN-CERT-2016-1410
dfn-cert: DFN-CERT-2016-1392
dfn-cert: DFN-CERT-2016-1387
dfn-cert: DFN-CERT-2016-1328
dfn-cert: DFN-CERT-2016-1167
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:

Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight

The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108368
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

Vulnerability Insight

The flaw is due to error in 'Sound' component.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.

Details: `Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux`

OID:1.3.6.1.4.1.25623.1.0.814408

Version used: `2022-06-29T10:11:11Z`

Product Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

Vulnerability Insight

The flaw is due to error in 'Sound' component.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Check if a vulnerable version is present on the target host.
Details: `Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux`
OID:1.3.6.1.4.1.25623.1.0.814408
Version used: `2022-06-29T10:11:11Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to a denial-of-service vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial-of-service condition.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier on Linux.

Vulnerability Insight
The flaw exists due to an error in the 'Serialization' sub-component of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 01 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108368
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2657
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0808
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE is prone to a denial of service (DoS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
path / port:        /usr/bin/java
```

Impact

Successful exploitation will allow attackers to cause partial denial of service conditions.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.6.0 to 1.6.0.201, 1.7.0 to 1.7.0.191, 1.8.0 to 1.8.0.182 on Linux.

Vulnerability Insight

The flaw is due to error in 'Sound' component.

Vulnerability Detection Method

Check if a vulnerable version is present on the target host.

Details: `Oracle Java SE Denial of Service Vulnerability(oct2018-4428296)-Linux`

OID:1.3.6.1.4.1.25623.1.0.814408

Version used: `2022-06-29T10:11:11Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-3214
url: http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
cert-bund: CB-K19/0175
cert-bund: CB-K18/1010
dfn-cert: DFN-CERT-2019-0413
dfn-cert: DFN-CERT-2019-0076
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2107
```

Medium (CVSS: 5.3)

NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108384
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2016-3458
cve: CVE-2016-3485
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-2041
dfn-cert: DFN-CERT-2016-1449
dfn-cert: DFN-CERT-2016-1448
dfn-cert: DFN-CERT-2016-1410
dfn-cert: DFN-CERT-2016-1392
dfn-cert: DFN-CERT-2016-1387
dfn-cert: DFN-CERT-2016-1328
dfn-cert: DFN-CERT-2016-1167
```

Medium (CVSS: 5.3)
NVT: Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple unspecified vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

. . . continues on next page . . .

. . . continued from previous page . . .

Successful exploitation will allow remote user to access and modify data on the target system, can cause denial of service conditions on the target system, a remote or local user can obtain elevated privileges on the target system, also a local user can modify data on the target system.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 6 update 115 and prior, 7 update 101 and prior, and 8 update 92 and prior on Linux.

Vulnerability Insight
Multiple flaws are due to:
- A flaw in the Hotspot component.
- A flaw in the Install component.
- A flaw in the JAXP component.
- A flaw in the CORBA component.
- A flaw in the Networking component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Multiple Unspecified Vulnerabilities-01 July 2016 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108384
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References
```
cve: CVE-2016-3458
cve: CVE-2016-3485
cve: CVE-2016-3500
cve: CVE-2016-3503
cve: CVE-2016-3508
cve: CVE-2016-3550
url: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
url: http://www.securityfocus.com/bid/91945
url: http://www.securityfocus.com/bid/91996
url: http://www.securityfocus.com/bid/91972
url: http://www.securityfocus.com/bid/91951
cert-bund: CB-K16/1993
cert-bund: CB-K16/1935
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1364
cert-bund: CB-K16/1363
cert-bund: CB-K16/1323
cert-bund: CB-K16/1308
cert-bund: CB-K16/1304
cert-bund: CB-K16/1251
cert-bund: CB-K16/1099
dfn-cert: DFN-CERT-2016-2104
dfn-cert: DFN-CERT-2016-2041
dfn-cert: DFN-CERT-2016-1449
dfn-cert: DFN-CERT-2016-1448
dfn-cert: DFN-CERT-2016-1410
dfn-cert: DFN-CERT-2016-1392
dfn-cert: DFN-CERT-2016-1387
dfn-cert: DFN-CERT-2016-1328
dfn-cert: DFN-CERT-2016-1167
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary
Oracle Java SE JRE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow attackers to disclose sensitive information.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight
The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.108426
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE JRE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to disclose sensitive information.

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight

The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108426

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 5.0)
NVT: Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Oracle Java SE JRE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow attackers to disclose sensitive information.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE 5.0u71 and prior, 6u81 and prior, and 7u67 and prior on Linux.

Vulnerability Insight

The flaw exists due to an error related to C2 optimizations and range checks in the Hotspot subcomponent.

Vulnerability Detection Method

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

Details: `Oracle Java SE JRE Unspecified Vulnerability-05 Oct 2014 (Linux)`

OID:1.3.6.1.4.1.25623.1.0.108426

Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2014-6504
url: http://secunia.com/advisories/61609/
url: http://www.securityfocus.com/bid/70564
url: http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
cert-bund: CB-K15/0393
cert-bund: CB-K14/1479
cert-bund: CB-K14/1295
cert-bund: CB-K14/1287
dfn-cert: DFN-CERT-2015-0404
dfn-cert: DFN-CERT-2014-1564
dfn-cert: DFN-CERT-2014-1356
dfn-cert: DFN-CERT-2014-1346
```

Medium (CVSS: 4.8)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to:

- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`

OID:1.3.6.1.4.1.25623.1.0.108370

Version used: `2022-05-19T11:50:09Z`

... continues on next page ...

. . . continued from previous page . . .

Product Detection Result

Product: cpe:/a:oracle:jdk:1.6.0:update_41

Method: Multiple Java Products Version Detection (Linux)

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 4.8)

NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact
Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:
Solution type: VendorFix
Apply the patch from the referenced advisory.

Affected Software/OS
Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

Vulnerability Insight
Multiple flaws exist due to:
- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108370
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 4.8)
NVT: Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to multiple vulnerabilities.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact

Successful exploitation of this vulnerability will allow remote attackers to conduct a denial of service condition, access data, partially modify data and gain elevated privileges.

Solution:

Solution type: VendorFix

Apply the patch from the referenced advisory.

Affected Software/OS

Oracle Java SE version 1.6.0.171 and earlier, 1.7.0.161 and earlier, 1.8.0.152 and earlier, 9.0.1 and earlier on Linux.

Vulnerability Insight

Multiple flaws exist due to:
- Multiple errors in 'Libraries' sub-component.
- Multiple errors in 'JNDI' sub-component.
- An error in 'JMX' sub-component.
- Multiple errors in 'AWT' sub-component.
- An error in 'JCE' sub-component.
- An error in 'JGSS' sub-component.
- An error in 'I18n' sub-component.
- An error in 'LDAP' sub-component.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (jan2018-3236628) 03 - Linux`
OID:1.3.6.1.4.1.25623.1.0.108370
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2677
cve: CVE-2018-2599
cve: CVE-2018-2603
cve: CVE-2018-2641
cve: CVE-2018-2602
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2018-2629
cve: CVE-2018-2678
cve: CVE-2018-2663
cve: CVE-2018-2633
cve: CVE-2018-2588
cve: CVE-2018-2637
cve: CVE-2018-2618
cve: CVE-2018-2579
url: http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
cert-bund: CB-K18/0882
cert-bund: CB-K18/0808
cert-bund: CB-K18/0715
cert-bund: CB-K18/0714
cert-bund: CB-K18/0689
cert-bund: CB-K18/0636
cert-bund: CB-K18/0091
dfn-cert: DFN-CERT-2019-0618
dfn-cert: DFN-CERT-2018-1915
dfn-cert: DFN-CERT-2018-1746
dfn-cert: DFN-CERT-2018-1703
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1078
dfn-cert: DFN-CERT-2018-1073
dfn-cert: DFN-CERT-2018-1000
dfn-cert: DFN-CERT-2018-0816
dfn-cert: DFN-CERT-2018-0645
dfn-cert: DFN-CERT-2018-0102
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /var/www/html/phpmyadmin/js/jquery/jquery-1.6.2.js
```

Solution:

Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

Product Detection Result

Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.4.4
Fixed version:     1.6.3
Installation
path / port:       /var/www/html/drupal/misc/jquery.js
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References
```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪rdoc/generator/template/sdoc/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result

```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.3.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     1.6.3
Installation
path / port:       /opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sdoc-0.4.1/lib/
↪rdoc/generator/template/rails/resources/js/jquery-1.3.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References
```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Product detection result
```
cpe:/a:jquery:jquery:1.6.2
Detected by jQuery Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.150658)
```

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /opt/chef/embedded/lib/ruby/gems/2.4.0/gems/simplecov-html-0.
↪10.2/assets/javascripts/libraries/jquery-1.6.2.min.js
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

Product Detection Result
Product: `cpe:/a:jquery:jquery:1.6.2`
Method: `jQuery Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.150658)

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
```

Impact
Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:
Solution type: VendorFix
Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS
Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight
The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813312
Version used: `2022-05-19T11:50:09Z`

Product Detection Result
Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/lib/jvm/java-6-openjdk-amd64/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux`
OID:1.3.6.1.4.1.25623.1.0.813312
Version used: `2022-05-19T11:50:09Z`

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`
Method: `Multiple Java Products Version Detection (Linux)`
OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

Medium (CVSS: 4.2)
NVT: Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux

Product detection result

```
cpe:/a:oracle:jdk:1.6.0:update_41
Detected by Multiple Java Products Version Detection (Linux) (OID: 1.3.6.1.4.1.2
↪5623.1.0.800385)
```

Summary

Oracle Java SE is prone to an unspecified vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.0update_41
Fixed version:     Apply the patch
Installation
path / port:       /usr/bin/java
```

Impact

Successful exploitation will allow remote attackers to affect confidentiality and integrity via unknown vectors.

Solution:

Solution type: VendorFix

Apply the appropriate patch from the vendor. Please see the references for more information.

Affected Software/OS

Oracle Java SE version 1.8.0.162 and earlier, 1.7.0.171 and earlier, 1.6.0.181 and earlier on Linux.

Vulnerability Insight

The flaw is due to an unspecified error in 'RMI' component of Java SE.

Vulnerability Detection Method

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

Details: `Oracle Java SE Security Updates (apr2018-3678067) 06 - Linux`

OID:1.3.6.1.4.1.25623.1.0.813312

Version used: `2022-05-19T11:50:09Z`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:oracle:jdk:1.6.0:update_41`

Method: `Multiple Java Products Version Detection (Linux)`

OID: 1.3.6.1.4.1.25623.1.0.800385)

References

```
cve: CVE-2018-2800
url: http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
cert-bund: WID-SEC-2023-1375
cert-bund: CB-K18/0808
cert-bund: CB-K18/0732
cert-bund: CB-K18/0600
dfn-cert: DFN-CERT-2018-1145
dfn-cert: DFN-CERT-2018-0724
```

[return to 10.0.0.10]

2.1.8 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/set
↪up/../js/jquery/jquery-1.6.2.js
- Referenced at:   http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/set
↪up/
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

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

Details: `jQuery < 1.9.0 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141636

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/js/
↪jquery/jquery-1.6.2.js
- Referenced at:   http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/
```

Solution:

Solution type: VendorFix

Update to version 1.9.0 or later.

Affected Software/OS

jQuery prior to version 1.9.0.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.0)
NVT: Sensitive File Disclosure (HTTP)

Summary

The script attempts to identify files containing sensitive data at the remote web server like e.g.:
- software (Blog, CMS) configuration or log files
- web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...)
- Cloud (e.g. AWS) configuration files
- database backup files
- SSH or SSL/TLS Private-Keys

Vulnerability Detection Result

```
The following files containing sensitive information were identified:
Description:   Microsoft IIS / ASP.NET Core Module web.config file accessible. T
↪his could contain sensitive information about the structure of the application
↪ / web server and shouldn't be accessible.
Match:         <configuration>
  <system.webServer>
Used regex:    ^\s*<(configuration|system\.web(Server)?)>
Extra match 1:   </system.webServer>
</configuration>
Used regex:    ^\s*</(configuration|system\.web(Server)?)>
URL:           http://ip-10-0-0-10.us-east-2.compute.internal/drupal/web.config
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact

Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

Solution:

Solution type: Mitigation

The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Detection Method

Enumerate the remote web server and check if sensitive files are accessible.

Details: `Sensitive File Disclosure (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.107305

Version used: `2023-05-23T11:14:48Z`

Medium (CVSS: 5.0)

NVT: Drupal 7.0 Information Disclosure Vulnerability - Active Check

Summary

Drupal is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Vulnerable URL: http://ip-10-0-0-10.us-east-2.compute.internal/drupal/modules/si
↪mpletest/tests/upgrade/drupal-6.upload.database.php
```

Impact

Successful exploitation will allow attacker to obtain sensitive information that could aid in further attacks.

Solution:

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

Drupal version 7.0 is known to be affected.

Vulnerability Insight

The flaw is due to insufficient error checking, allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Drupal 7.0 Information Disclosure Vulnerability - Active Check`
OID:1.3.6.1.4.1.25623.1.0.902574
Version used: `2021-12-01T11:10:56Z`

References

```
cve: CVE-2011-3730
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/!_README
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/drupal-7.0
```

Medium (CVSS: 5.0)
NVT: Unprotected Web App / Device Installers (HTTP)

Summary

The script attempts to identify installation/setup pages of various web apps/devices that are publicly accessible and not protected by e.g. account restrictions or having their setup finished.

Vulnerability Detection Result

```
The following web app/device installers are unprotected/have not finished their
↪setup and are publicly accessible (URL:Description):
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/setup/index.php - Cube
↪Cart / phpMyAdmin installer
```

Impact

It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

Solution:

Solution type: Mitigation

Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it, remove it completely or finish the setup of the application / device.

Vulnerability Detection Method

Enumerate the remote web server and check if unprotected web apps/devices are accessible for installation.

Details: `Unprotected Web App / Device Installers (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107307
Version used: `2023-06-01T09:09:48Z`

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

Summary

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://ip-10-0-0-10.us-east-2.compute.internal/drupal/:pass
http://ip-10-0-0-10.us-east-2.compute.internal/drupal/?D=A:pass
http://ip-10-0-0-10.us-east-2.compute.internal/payroll_app.php:password
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/:pma_password
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/?D=A:pma_password
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/changelog.php:pma_pass
↪word
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/index.php:pma_password
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/license.php:pma_passwo
↪rd
http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/url.php:pma_password
```

Impact

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

Solution:

Solution type: Workaround

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

Affected Software/OS

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

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440

Version used: `2020-08-24T15:18:35Z`

References

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

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/set
↪up/../js/jquery/jquery-1.6.2.js
- Referenced at:   http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/set
↪up/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/js/
↪jquery/jquery-1.6.2.js
- Referenced at:   http://ip-10-0-0-10.us-east-2.compute.internal/phpmyadmin/
```

Solution:

Solution type: VendorFix

Update to version 1.6.3 or later.

Affected Software/OS

jQuery prior to version 1.6.3.

Vulnerability Insight

Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method

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

Details: `jQuery < 1.6.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.141637

Version used: `2023-07-14T05:06:08Z`

References

```
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

[return to 10.0.0.10]

2.1.9 Medium package

Medium (CVSS: 6.9)

NVT: Ubuntu: Security Advisory (USN-2204-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-2204-1 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   linux-image-3.13.0-24-generic
Installed version:    linux-image-3.13.0-24-generic-3.13.0-24.46
Fixed version:      >=linux-image-3.13.0-24-generic-3.13.0-24.47
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
A flaw was discovered in the Linux kernel's pseudo tty (pty) device. An unprivileged user could exploit this flaw to cause a denial of service (system crash) or potentially gain administrator privileges.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-2204-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2014.2204.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-2204-1
cve: CVE-2014-0196
advisory_id: USN-2204-1
cert-bund: CB-K14/0807
cert-bund: CB-K14/0757
cert-bund: CB-K14/0722
cert-bund: CB-K14/0646
cert-bund: CB-K14/0638
cert-bund: CB-K14/0627
cert-bund: CB-K14/0610
cert-bund: CB-K14/0599
cert-bund: CB-K14/0597
cert-bund: CB-K14/0576
cert-bund: CB-K14/0575
cert-bund: CB-K14/0557
cert-bund: CB-K14/0543
cert-bund: CB-K14/0528
dfn-cert: DFN-CERT-2014-0841
dfn-cert: DFN-CERT-2014-0787
dfn-cert: DFN-CERT-2014-0752
dfn-cert: DFN-CERT-2014-0672
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2014-0663
dfn-cert: DFN-CERT-2014-0644
dfn-cert: DFN-CERT-2014-0637
dfn-cert: DFN-CERT-2014-0623
dfn-cert: DFN-CERT-2014-0622
dfn-cert: DFN-CERT-2014-0604
dfn-cert: DFN-CERT-2014-0600
dfn-cert: DFN-CERT-2014-0582
dfn-cert: DFN-CERT-2014-0569
dfn-cert: DFN-CERT-2014-0549
```

Medium (CVSS: 6.8)
NVT: Ubuntu: Security Advisory (USN-4931-1)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4931-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm11
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 14.04.

Vulnerability Insight
Steven French discovered that Samba incorrectly handled ChangeNotify permissions. A remote attacker could possibly use this issue to obtain file name information. (CVE-2020-14318)
Bas Alberts discovered that Samba incorrectly handled certain winbind requests. A remote attacker could possibly use this issue to cause winbind to crash, resulting in a denial of service. (CVE-2020-14323)
Francis Brosnan Blazquez discovered that Samba incorrectly handled certain invalid DNS records. A remote attacker could possibly use this issue to cause the DNS server to crash, resulting in a denial of service. (CVE-2020-14383)
Peter Eriksson discovered that Samba incorrectly handled certain negative idmap cache entries. This issue could result in certain users gaining unauthorized access to files, contrary to expected behaviour. (CVE-2021-20254)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4931-1)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2021.4931.1
Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4931-1
cve: CVE-2020-14318
cve: CVE-2020-14323
cve: CVE-2020-14383
cve: CVE-2021-20254
advisory_id: USN-4931-1
cert-bund: WID-SEC-2023-0174
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-0530
cert-bund: CB-K22/0130
cert-bund: CB-K21/0451
cert-bund: CB-K20/1051
dfn-cert: DFN-CERT-2023-0153
dfn-cert: DFN-CERT-2022-1469
dfn-cert: DFN-CERT-2022-0332
dfn-cert: DFN-CERT-2022-0224
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2021-2438
dfn-cert: DFN-CERT-2021-2072
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1167
dfn-cert: DFN-CERT-2021-0929
dfn-cert: DFN-CERT-2021-0906
dfn-cert: DFN-CERT-2021-0902
dfn-cert: DFN-CERT-2021-0444
dfn-cert: DFN-CERT-2020-2749
dfn-cert: DFN-CERT-2020-2567
dfn-cert: DFN-CERT-2020-2346
```

Medium (CVSS: 6.8)
NVT: Ubuntu: Security Advisory (USN-3445-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-3445-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.133.142
```

Solution:

Solution type: VendorFix

. . . continues on next page . . .

... continued from previous page ...

Please install the updated package(s).

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

Eyal Itkin discovered that the IP over IEEE 1394 (FireWire) implementation in the Linux kernel contained a buffer overflow when handling fragmented packets. A remote attacker could use this to possibly execute arbitrary code with administrative privileges. (CVE-2016-8633)

Andrey Konovalov discovered that a divide-by-zero error existed in the TCP stack implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash). (CVE-2017-14106)

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3445-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2017.3445.1

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3445-1
cve: CVE-2016-8633
cve: CVE-2017-14106
advisory_id: USN-3445-1
cert-bund: CB-K18/0364
cert-bund: CB-K18/0153
cert-bund: CB-K18/0066
cert-bund: CB-K18/0049
cert-bund: CB-K18/0017
cert-bund: CB-K17/2169
cert-bund: CB-K17/1952
cert-bund: CB-K17/1908
cert-bund: CB-K17/1867
cert-bund: CB-K17/1849
cert-bund: CB-K17/1840
cert-bund: CB-K17/1813
cert-bund: CB-K17/1776
cert-bund: CB-K17/1708
cert-bund: CB-K17/1607
cert-bund: CB-K17/1567
cert-bund: CB-K17/0838
cert-bund: CB-K17/0697
cert-bund: CB-K17/0552
cert-bund: CB-K17/0297
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: CB-K17/0238
cert-bund: CB-K17/0212
cert-bund: CB-K17/0168
cert-bund: CB-K16/1999
cert-bund: CB-K16/1913
cert-bund: CB-K16/1911
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1374
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0669
dfn-cert: DFN-CERT-2018-0392
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0077
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2017-2269
dfn-cert: DFN-CERT-2017-2042
dfn-cert: DFN-CERT-2017-1993
dfn-cert: DFN-CERT-2017-1949
dfn-cert: DFN-CERT-2017-1930
dfn-cert: DFN-CERT-2017-1922
dfn-cert: DFN-CERT-2017-1893
dfn-cert: DFN-CERT-2017-1852
dfn-cert: DFN-CERT-2017-1787
dfn-cert: DFN-CERT-2017-1678
dfn-cert: DFN-CERT-2017-1637
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0171
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-2024
```

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory (USN-4249-1)

Summary
The remote host is missing an update for the 'e2fsprogs' package(s) announced via the USN-4249-1 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   e2fsprogs
Installed version:    e2fsprogs-1.42.9-3ubuntu1.2
Fixed version:      >=e2fsprogs-1.42.9-3ubuntu1.3+esm2
```

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

Affected Software/OS
'e2fsprogs' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that e2fsprogs incorrectly handled certain ext4 partitions. 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-4249-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4249.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4249-1
cve: CVE-2019-5188
advisory_id: USN-4249-1
cert-bund: CB-K20/1030
cert-bund: CB-K20/0109
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-0113
dfn-cert: DFN-CERT-2020-0065
```

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory (USN-4142-2)

Summary
The remote host is missing an update for the 'e2fsprogs' package(s) announced via the USN-4142-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   e2fsprogs
Installed version:    e2fsprogs-1.42.9-3ubuntu1.2
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=e2fsprogs-1.42.9-3ubuntu1.3+esm1
```

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

Affected Software/OS
'e2fsprogs' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4142-1 fixed a vulnerability in e2fsprogs. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that e2fsprogs incorrectly handled certain ext4 partitions. 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-4142-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4142.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4142-2
cve: CVE-2019-5094
advisory_id: USN-4142-2
cert-bund: CB-K20/1049
cert-bund: CB-K20/1030
cert-bund: CB-K20/0845
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-0113
dfn-cert: DFN-CERT-2019-2024
```

Medium (CVSS: 6.7)
NVT: Ubuntu: Security Advisory (USN-3908-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3908-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.166.177
```

. . . continues on next page . . .

... continued from previous page ...

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Jann Horn discovered a race condition in the fork() system call in the Linux kernel. A local attacker could use this to gain access to services that cache authorizations.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3908-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3908.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3908-1
cve: CVE-2019-6133
advisory_id: USN-3908-1
cert-bund: CB-K19/0103
dfn-cert: DFN-CERT-2021-0329
dfn-cert: DFN-CERT-2020-2592
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1405
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-0547
dfn-cert: DFN-CERT-2019-0470
dfn-cert: DFN-CERT-2019-0462
dfn-cert: DFN-CERT-2019-0181
dfn-cert: DFN-CERT-2019-0050
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5520-2)

Summary
The remote host is missing an update for the 'libhttp-daemon-perl' package(s) announced via the USN-5520-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libhttp-daemon-perl
Installed version:    libhttp-daemon-perl-6.01-1
Fixed version:      >=libhttp-daemon-perl-6.01-1ubuntu0.14.04~esm1
```

... continues on next page ...

. . . continued from previous page . . .

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

Affected Software/OS
'libhttp-daemon-perl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5520-1 fixed a vulnerability in HTTP-Daemon. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5520-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5520.2
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-5520-2
cve: CVE-2022-31081
advisory_id: USN-5520-2
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-5742-1)

Summary
The remote host is missing an update for the 'jbigkit' package(s) announced via the USN-5742-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjbig0
Installed version:    libjbig0-2.0-2ubuntu4.1
Fixed version:      >=libjbig0-2.0-2ubuntu4.1+esm1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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.

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: `2022-11-25T04:10:30Z`

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-4167-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4167-2 advisory.

Vulnerability Detection Result
```
Vulnerable package:   libsmbclient
Installed version:    libsmbclient-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=libsmbclient-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm3
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm3
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 12.04, Ubuntu 14.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-4167-1 fixed several vulnerabilities in Samba. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Michael Hanselmann discovered that the Samba client code incorrectly handled path separators. If a user were tricked into connecting to a malicious server, a remote attacker could use this issue to cause the client to access local pathnames instead of network pathnames. (CVE-2019-10218)
Adam Xu discovered that Samba incorrectly handled the dirsync LDAP control. A remote attacker with 'get changes' permissions could possibly use this issue to cause Samba to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 ESM. (CVE-2019-14847)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4167-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4167.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4167-2
cve: CVE-2019-10218
cve: CVE-2019-14847
advisory_id: USN-4167-2
cert-bund: CB-K19/0945
dfn-cert: DFN-CERT-2021-1167
dfn-cert: DFN-CERT-2020-2026
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2020-0891
dfn-cert: DFN-CERT-2020-0657
dfn-cert: DFN-CERT-2020-0600
dfn-cert: DFN-CERT-2020-0375
dfn-cert: DFN-CERT-2019-2244
dfn-cert: DFN-CERT-2019-2240
```

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.

Vulnerability Detection Result

```
Vulnerable package:   dbus
Installed version:    dbus-1.6.18-0ubuntu4.4
Fixed version:      >=dbus-1.6.18-0ubuntu4.5+esm3
Vulnerable package:   libdbus-1-3
Installed version:    libdbus-1-3-1.6.18-0ubuntu4.4
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=libdbus-1-3-1.6.18-0ubuntu4.5+esm3
```

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
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: `2022-10-28T04:26:19Z`

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-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-4187-1)

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is missing an update for the 'linux' package(s) announced via the USN-4187-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.175.186
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Giorgi Maisuradze, Moritz Lipp, Michael Schwarz, Daniel Gruss, and Jo Van Bulck discovered that Intel processors using Transactional Synchronization Extensions (TSX) could expose memory contents previously stored in microarchitectural buffers to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4187-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4187.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4187-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/TAA_MCEPSC_i915
cve: CVE-2019-11135
advisory_id: USN-4187-1
cert-bund: WID-SEC-2023-1689
cert-bund: WID-SEC-2023-0884
cert-bund: CB-K19/0980
cert-bund: CB-K19/0978
dfn-cert: DFN-CERT-2020-1711
dfn-cert: DFN-CERT-2020-0466
dfn-cert: DFN-CERT-2020-0333
dfn-cert: DFN-CERT-2020-0269
dfn-cert: DFN-CERT-2020-0253
dfn-cert: DFN-CERT-2020-0078
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2019-2644
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-2640
dfn-cert: DFN-CERT-2019-2582
dfn-cert: DFN-CERT-2019-2568
dfn-cert: DFN-CERT-2019-2560
dfn-cert: DFN-CERT-2019-2450
dfn-cert: DFN-CERT-2019-2421
dfn-cert: DFN-CERT-2019-2407
dfn-cert: DFN-CERT-2019-2402
dfn-cert: DFN-CERT-2019-2399
dfn-cert: DFN-CERT-2019-2397
dfn-cert: DFN-CERT-2019-2392
dfn-cert: DFN-CERT-2019-2390
dfn-cert: DFN-CERT-2019-2389
dfn-cert: DFN-CERT-2019-2388
dfn-cert: DFN-CERT-2019-2387
dfn-cert: DFN-CERT-2019-2386
dfn-cert: DFN-CERT-2019-2385
dfn-cert: DFN-CERT-2019-2384
dfn-cert: DFN-CERT-2019-2383
dfn-cert: DFN-CERT-2019-2382
dfn-cert: DFN-CERT-2019-2381
dfn-cert: DFN-CERT-2019-2379
dfn-cert: DFN-CERT-2019-2378
dfn-cert: DFN-CERT-2019-2375
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-2372
dfn-cert: DFN-CERT-2019-2370
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libaprutil1
Installed version:    libaprutil1-1.5.3-1
Fixed version:      >=libaprutil1-1.5.3-1ubuntu0.1~esm2
```

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

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Insight

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

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5870-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5870.1
Version used: `2023-05-19T04:09:46Z`

References

```
url: https://ubuntu.com/security/notices/USN-5870-1
cve: CVE-2022-25147
advisory_id: USN-5870-1
cert-bund: WID-SEC-2023-1424
cert-bund: WID-SEC-2023-0245
dfn-cert: DFN-CERT-2023-1297
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-6229-1)

Summary

The remote host is missing an update for the 'tiff' package(s) announced via the USN-6229-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm8
```

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.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that LibTIFF was not properly handling variables used to perform memory management operations when processing an image through tiffcrop, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. (CVE-2023-25433, CVE-2023-26965)
It was discovered that LibTIFF was not properly processing numerical values when dealing with little-endian input data, which could lead to the execution of an invalid operation. An attacker could possibly use this issue to cause a denial of service (CVE-2023-26966)
It was discovered that LibTIFF was not properly performing bounds checks when closing a previously opened TIFF file, which could lead to a NULL pointer dereference. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-3316)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6229-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6229.1
Version used: `2023-07-14T04:09:48Z`

References

```
url: https://ubuntu.com/security/notices/USN-6229-1
cve: CVE-2023-25433
cve: CVE-2023-26965
cve: CVE-2023-26966
cve: CVE-2023-3316
advisory_id: USN-6229-1
cert-bund: WID-SEC-2023-1613
cert-bund: WID-SEC-2023-1514
cert-bund: WID-SEC-2023-1479
dfn-cert: DFN-CERT-2023-1608
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-4593-2)

Summary
The remote host is missing an update for the 'freetype' package(s) announced via the USN-4593-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libfreetype6
Installed version:    libfreetype6-2.5.2-1ubuntu2.8
Fixed version:      >=libfreetype6-2.5.2-1ubuntu2.8+esm2
```

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

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

'freetype' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-4593-1 fixed a vulnerability in FreeType. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Sergei Glazunov 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 with user privileges.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4593-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4593.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4593-2
cve: CVE-2020-15999
advisory_id: USN-4593-2
cert-bund: WID-SEC-2022-1994
cert-bund: CB-K21/0007
cert-bund: CB-K20/1145
cert-bund: CB-K20/1010
cert-bund: CB-K20/1004
dfn-cert: DFN-CERT-2021-1706
dfn-cert: DFN-CERT-2021-0781
dfn-cert: DFN-CERT-2021-0186
dfn-cert: DFN-CERT-2021-0010
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2626
dfn-cert: DFN-CERT-2020-2588
dfn-cert: DFN-CERT-2020-2538
dfn-cert: DFN-CERT-2020-2528
dfn-cert: DFN-CERT-2020-2527
dfn-cert: DFN-CERT-2020-2285
dfn-cert: DFN-CERT-2020-2280
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-4333-1)

Summary

The remote host is missing an update for the 'python2.7, python3.4, python3.5, python3.6, python3.7' package(s) announced via the USN-4333-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python2.7
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    python2.7-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-2.7.6-8ubuntu0.6+esm5
Vulnerable package:   python2.7-minimal
Installed version:    python2.7-minimal-2.7.6-8ubuntu0.5
Fixed version:      >=python2.7-minimal-2.7.6-8ubuntu0.6+esm5
Vulnerable package:   python3.4
Installed version:    python3.4-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-3.4.3-1ubuntu1~14.04.7+esm6
Vulnerable package:   python3.4-minimal
Installed version:    python3.4-minimal-3.4.3-1ubuntu1~14.04.7
Fixed version:      >=python3.4-minimal-3.4.3-1ubuntu1~14.04.7+esm6
```

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

Affected Software/OS
'python2.7, python3.4, python3.5, python3.6, python3.7' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.10.

Vulnerability Insight
It was discovered that Python incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. (CVE-2019-18348)
It was discovered that Python incorrectly handled certain HTTP requests. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-8492)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4333-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4333.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4333-1
cve: CVE-2019-18348
cve: CVE-2020-8492
advisory_id: USN-4333-1
cert-bund: WID-SEC-2022-2191
cert-bund: WID-SEC-2022-2190
cert-bund: CB-K22/0130
cert-bund: CB-K20/1030
cert-bund: CB-K20/1028
dfn-cert: DFN-CERT-2023-1200
dfn-cert: DFN-CERT-2022-2715
dfn-cert: DFN-CERT-2022-0224
dfn-cert: DFN-CERT-2021-2648
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0553
dfn-cert: DFN-CERT-2021-0533
dfn-cert: DFN-CERT-2020-2805
dfn-cert: DFN-CERT-2020-2757
dfn-cert: DFN-CERT-2020-2621
dfn-cert: DFN-CERT-2020-2392
dfn-cert: DFN-CERT-2020-2386
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2278
dfn-cert: DFN-CERT-2020-2117
dfn-cert: DFN-CERT-2020-1812
dfn-cert: DFN-CERT-2020-1540
dfn-cert: DFN-CERT-2020-1405
dfn-cert: DFN-CERT-2020-1168
dfn-cert: DFN-CERT-2020-0694
dfn-cert: DFN-CERT-2020-0597
dfn-cert: DFN-CERT-2020-0438
dfn-cert: DFN-CERT-2020-0395
dfn-cert: DFN-CERT-2019-2252
```

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.

Vulnerability Detection Result

```
Vulnerable package:   libxml2
Installed version:    libxml2-2.9.1+dfsg1-3ubuntu4.13
Fixed version:      >=libxml2-2.9.1+dfsg1-3ubuntu4.13+esm5
```

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)

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash. (CVE-2023-29469)

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: `2023-05-08T04:09:30Z`

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-2023-1614
cert-bund: WID-SEC-2023-0920
dfn-cert: DFN-CERT-2023-0969
dfn-cert: DFN-CERT-2023-0836
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5503-2)

Summary

The remote host is missing an update for the 'gnupg, gnupg2' package(s) announced via the USN-5503-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   gnupg
Installed version:    gnupg-1.4.16-1ubuntu2.6
Fixed version:      >=gnupg-1.4.16-1ubuntu2.6+esm1
```

Solution:

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

Affected Software/OS

'gnupg, gnupg2' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight

USN-5503-1 fixed a vulnerability in GnuPG. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
Demi Marie Obenour discovered that GnuPG incorrectly handled injection in the status message. A remote attacker could possibly use this issue to forge signatures.

. . . 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-5503-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5503.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5503-2
cve: CVE-2022-34903
advisory_id: USN-5503-2
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-4616-2)

Summary

The remote host is missing an update for the 'accountsservice' package(s) announced via the USN-4616-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   accountsservice
Installed version:    accountsservice-0.6.35-0ubuntu7
Fixed version:      >=accountsservice-0.6.35-0ubuntu7.3+esm2
Vulnerable package:   libaccountsservice0
Installed version:    libaccountsservice0-0.6.35-0ubuntu7
Fixed version:      >=libaccountsservice0-0.6.35-0ubuntu7.3+esm2
```

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

Affected Software/OS

'accountsservice' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-4616-1 fixed several vulnerabilities in AccountsService. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

Kevin Backhouse discovered that AccountsService incorrectly dropped privileges. A local user could possibly use this issue to cause AccountsService to crash or hang, resulting in a denial of service. (CVE-2020-16126)
Matthias Gerstner discovered that AccountsService incorrectly handled certain path checks. A local attacker could possibly use this issue to read arbitrary files. (CVE-2018-14036)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4616-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4616.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4616-2
cve: CVE-2018-14036
cve: CVE-2020-16126
advisory_id: USN-4616-2
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-2251
```

Medium (CVSS: 6.5)
NVT: Ubuntu: Security Advisory (USN-5658-3)

Summary
The remote host is missing an update for the 'isc-dhcp' package(s) announced via the USN-5658-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   isc-dhcp-client
Installed version:    isc-dhcp-client-4.2.4-7ubuntu12.12
Fixed version:      >=isc-dhcp-client-4.2.4-7ubuntu12.13+esm2
```

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

Affected Software/OS
'isc-dhcp' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-5658-1 fixed several vulnerabilities in DHCP. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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-5658-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5658.3
Version used: `2022-11-30T04:11:02Z`

References

```
url: https://ubuntu.com/security/notices/USN-5658-3
cve: CVE-2022-2928
cve: CVE-2022-2929
advisory_id: USN-5658-3
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: 6.3)
NVT: Ubuntu: Security Advisory (USN-4236-3)

Summary

The remote host is missing an update for the 'libgcrypt11' package(s) announced via the USN-4236-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libgcrypt11
Installed version:    libgcrypt11-1.5.3-2ubuntu4.6
Fixed version:      >=libgcrypt11-1.5.3-2ubuntu4.6+esm1
```

Solution:

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

Affected Software/OS

'libgcrypt11' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4236-1 fixed a vulnerability in Libgcrypt. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that Libgcrypt was susceptible to a ECDSA timing attack. An attacker could possibly use this attack to recover sensitive information.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4236-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4236.3
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4236-3
cve: CVE-2019-13627
advisory_id: USN-4236-3
cert-bund: WID-SEC-2022-0193
cert-bund: CB-K20/1076
dfn-cert: DFN-CERT-2021-1070
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2019-1885
```

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-3990-2)

Summary

The remote host is missing an update for the 'python-urllib3' package(s) announced via the USN-3990-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python-urllib3
Installed version:    python-urllib3-1.7.1-1ubuntu4.1
Fixed version:      >=python-urllib3-1.7.1-1ubuntu4.1+esm1
```

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

Affected Software/OS

'python-urllib3' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-3990-1 fixed a vulnerability in urllib3. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that urllib3 incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. (CVE-2019-11236)

. . . 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-3990-2)`

OID:1.3.6.1.4.1.25623.1.1.12.2019.3990.2

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3990-2
cve: CVE-2019-11236
advisory_id: USN-3990-2
cert-bund: WID-SEC-2022-0517
cert-bund: CB-K20/1049
cert-bund: CB-K19/0696
cert-bund: CB-K19/0612
dfn-cert: DFN-CERT-2021-1296
dfn-cert: DFN-CERT-2020-0896
dfn-cert: DFN-CERT-2020-0217
dfn-cert: DFN-CERT-2019-2310
dfn-cert: DFN-CERT-2019-2302
dfn-cert: DFN-CERT-2019-1854
dfn-cert: DFN-CERT-2019-1831
dfn-cert: DFN-CERT-2019-1638
dfn-cert: DFN-CERT-2019-1457
dfn-cert: DFN-CERT-2019-1256
dfn-cert: DFN-CERT-2019-0801
```

Medium (CVSS: 6.1)
NVT: Ubuntu: Security Advisory (USN-4509-1)

Summary

The remote host is missing an update for the 'libdbi-perl' package(s) announced via the USN-4509-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libdbi-perl
Installed version:    libdbi-perl-1.630-1
Fixed version:      >=libdbi-perl-1.630-1ubuntu0.1~esm4
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'libdbi-perl' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It was discovered that Perl DBI module incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. (CVE-2013-7490)
It was discovered that Perl DBI module incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information. (CVE-2014-10401)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4509-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4509.1
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4509-1
cve: CVE-2013-7490
cve: CVE-2014-10401
advisory_id: USN-4509-1
cert-bund: CB-K20/1149
dfn-cert: DFN-CERT-2020-2554
dfn-cert: DFN-CERT-2020-2176
dfn-cert: DFN-CERT-2020-2172
dfn-cert: DFN-CERT-2020-2019
```

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-4745-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-4745-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm2
```

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

Affected Software/OS
'openssl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
David Benjamin discovered that OpenSSL incorrectly handled comparing certificates containing a EDIPartyName name type. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2020-1971)

. . . continues on next page . . .

. . . continued from previous page . . .

Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer fields. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. (CVE-2021-23841)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4745-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4745.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4745-1
cve: CVE-2020-1971
cve: CVE-2021-23841
advisory_id: USN-4745-1
cert-bund: WID-SEC-2023-0067
cert-bund: WID-SEC-2023-0065
cert-bund: WID-SEC-2022-2047
cert-bund: WID-SEC-2022-1908
cert-bund: WID-SEC-2022-1303
cert-bund: WID-SEC-2022-1000
cert-bund: WID-SEC-2022-0676
cert-bund: WID-SEC-2022-0669
cert-bund: WID-SEC-2022-0602
cert-bund: WID-SEC-2022-0585
cert-bund: CB-K21/1065
cert-bund: CB-K21/0788
cert-bund: CB-K21/0615
cert-bund: CB-K21/0573
cert-bund: CB-K21/0572
cert-bund: CB-K21/0565
cert-bund: CB-K21/0421
cert-bund: CB-K21/0412
cert-bund: CB-K21/0389
cert-bund: CB-K21/0185
cert-bund: CB-K21/0111
cert-bund: CB-K21/0062
cert-bund: CB-K21/0006
cert-bund: CB-K20/1217
dfn-cert: DFN-CERT-2022-1582
dfn-cert: DFN-CERT-2022-1571
dfn-cert: DFN-CERT-2022-1215
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2394
dfn-cert: DFN-CERT-2021-2216
dfn-cert: DFN-CERT-2021-2214
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-2190
dfn-cert: DFN-CERT-2021-2126
dfn-cert: DFN-CERT-2021-1803
dfn-cert: DFN-CERT-2021-1670
dfn-cert: DFN-CERT-2021-1547
dfn-cert: DFN-CERT-2021-1504
dfn-cert: DFN-CERT-2021-1418
dfn-cert: DFN-CERT-2021-1225
dfn-cert: DFN-CERT-2021-1132
dfn-cert: DFN-CERT-2021-1129
dfn-cert: DFN-CERT-2021-1128
dfn-cert: DFN-CERT-2021-0924
dfn-cert: DFN-CERT-2021-0862
dfn-cert: DFN-CERT-2021-0828
dfn-cert: DFN-CERT-2021-0826
dfn-cert: DFN-CERT-2021-0821
dfn-cert: DFN-CERT-2021-0819
dfn-cert: DFN-CERT-2021-0818
dfn-cert: DFN-CERT-2021-0806
dfn-cert: DFN-CERT-2021-0740
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2021-0408
dfn-cert: DFN-CERT-2021-0379
dfn-cert: DFN-CERT-2021-0363
dfn-cert: DFN-CERT-2021-0338
dfn-cert: DFN-CERT-2021-0255
dfn-cert: DFN-CERT-2021-0134
dfn-cert: DFN-CERT-2021-0131
dfn-cert: DFN-CERT-2021-0128
dfn-cert: DFN-CERT-2021-0120
dfn-cert: DFN-CERT-2021-0107
dfn-cert: DFN-CERT-2021-0078
dfn-cert: DFN-CERT-2021-0012
dfn-cert: DFN-CERT-2020-2791
dfn-cert: DFN-CERT-2020-2668
```

Medium (CVSS: 5.9)
NVT: Ubuntu: Security Advisory (USN-5894-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-5894-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm14
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm14
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm14
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04, Ubuntu 16.04.

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. This issue was only fixed in Ubuntu 14.04 ESM. (CVE-2021-22898, CVE-2021-22925)
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-5894-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5894.1
Version used: `2023-02-28T04:10:38Z`

References

```
url: https://ubuntu.com/security/notices/USN-5894-1
cve: CVE-2021-22898
cve: CVE-2021-22925
cve: CVE-2022-43552
advisory_id: USN-5894-1
cert-bund: WID-SEC-2023-1614
cert-bund: WID-SEC-2023-1350
cert-bund: WID-SEC-2023-0777
cert-bund: WID-SEC-2022-2375
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-2023-1522
```

. . . continues on next page . . .

... continued from previous page ...

```
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-2023-0685
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
dfn-cert: DFN-CERT-2022-1892
dfn-cert: DFN-CERT-2022-1692
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-2021-1917
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: 5.9)
NVT: Ubuntu: Security Advisory (USN-4376-2)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-4376-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libssl1.0.0
Installed version:    libssl1.0.0-1.0.1f-1ubuntu2.27
Fixed version:      >=libssl1.0.0-1.0.1f-1ubuntu2.27+esm1
```

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

... continues on next page ...

. . . continued from previous page . . .

Affected Software/OS
'openssl' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4376-1 fixed several vulnerabilities in OpenSSL. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Cesar Pereida Garcia, Sohaib ul Hassan, Nicola Tuveri, Iaroslav Gridin, Alejandro Cabrera Aldaya, and Billy Brumley discovered that OpenSSL incorrectly handled ECDSA signatures. An attacker could possibly use this issue to perform a timing side-channel attack and recover private ECDSA keys. (CVE-2019-1547)
Juraj Somorovsky, Robert Merget, and Nimrod Aviram discovered that certain applications incorrectly used OpenSSL and could be exposed to a padding oracle attack. A remote attacker could possibly use this issue to decrypt data. (CVE-2019-1559)
Bernd Edlinger discovered that OpenSSL incorrectly handled certain decryption functions. In certain scenarios, a remote attacker could possibly use this issue to perform a padding oracle attack and decrypt traffic. (CVE-2019-1563)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4376-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4376.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4376-2
cve: CVE-2019-1547
cve: CVE-2019-1559
cve: CVE-2019-1563
advisory_id: USN-4376-2
cert-bund: WID-SEC-2023-1762
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2023-1049
cert-bund: WID-SEC-2022-0673
cert-bund: WID-SEC-2022-0462
cert-bund: CB-K22/0045
cert-bund: CB-K20/1049
cert-bund: CB-K20/1016
cert-bund: CB-K20/0321
cert-bund: CB-K20/0318
cert-bund: CB-K20/0043
cert-bund: CB-K20/0041
cert-bund: CB-K20/0038
cert-bund: CB-K20/0036
cert-bund: CB-K20/0028
cert-bund: CB-K19/1025
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K19/0919
cert-bund: CB-K19/0915
cert-bund: CB-K19/0911
cert-bund: CB-K19/0808
cert-bund: CB-K19/0639
cert-bund: CB-K19/0623
cert-bund: CB-K19/0622
cert-bund: CB-K19/0620
cert-bund: CB-K19/0619
cert-bund: CB-K19/0615
cert-bund: CB-K19/0332
cert-bund: CB-K19/0320
cert-bund: CB-K19/0319
cert-bund: CB-K19/0173
dfn-cert: DFN-CERT-2020-2189
dfn-cert: DFN-CERT-2020-2014
dfn-cert: DFN-CERT-2020-1729
dfn-cert: DFN-CERT-2020-0895
dfn-cert: DFN-CERT-2020-0776
dfn-cert: DFN-CERT-2020-0775
dfn-cert: DFN-CERT-2020-0772
dfn-cert: DFN-CERT-2020-0716
dfn-cert: DFN-CERT-2020-0277
dfn-cert: DFN-CERT-2020-0101
dfn-cert: DFN-CERT-2020-0096
dfn-cert: DFN-CERT-2020-0092
dfn-cert: DFN-CERT-2020-0091
dfn-cert: DFN-CERT-2020-0090
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2457
dfn-cert: DFN-CERT-2019-2164
dfn-cert: DFN-CERT-2019-2158
dfn-cert: DFN-CERT-2019-2157
dfn-cert: DFN-CERT-2019-2149
dfn-cert: DFN-CERT-2019-2046
dfn-cert: DFN-CERT-2019-1996
dfn-cert: DFN-CERT-2019-1900
dfn-cert: DFN-CERT-2019-1897
dfn-cert: DFN-CERT-2019-1755
dfn-cert: DFN-CERT-2019-1746
dfn-cert: DFN-CERT-2019-1722
dfn-cert: DFN-CERT-2019-1678
dfn-cert: DFN-CERT-2019-1677
dfn-cert: DFN-CERT-2019-1617
dfn-cert: DFN-CERT-2019-1486
dfn-cert: DFN-CERT-2019-1460
dfn-cert: DFN-CERT-2019-1455
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1453
dfn-cert: DFN-CERT-2019-1450
dfn-cert: DFN-CERT-2019-1408
dfn-cert: DFN-CERT-2019-1240
dfn-cert: DFN-CERT-2019-0781
dfn-cert: DFN-CERT-2019-0775
dfn-cert: DFN-CERT-2019-0771
dfn-cert: DFN-CERT-2019-0566
dfn-cert: DFN-CERT-2019-0556
dfn-cert: DFN-CERT-2019-0412
```

Medium (CVSS: 5.7)
NVT: Ubuntu: Security Advisory (USN-4667-2)

Summary
The remote host is missing an update for the 'apt' package(s) announced via the USN-4667-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   apt
Installed version:    apt-1.0.1ubuntu2.19
Fixed version:      >=apt-1.0.1ubuntu2.24+esm3
```

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

Affected Software/OS
'apt' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4667-1 fixed a vulnerability in APT. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Kevin Backhouse discovered that APT incorrectly handled certain packages. A local attacker could possibly use this issue to cause APT to crash or 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-4667-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4667.2
Version used: `2022-09-13T14:14:11Z`

References
`url: https://ubuntu.com/security/notices/USN-4667-2`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-27350
advisory_id: USN-4667-2
cert-bund: CB-K20/1227
dfn-cert: DFN-CERT-2020-2689
```

Medium (CVSS: 5.6)
NVT: Ubuntu: Security Advisory (USN-3983-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3983-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.170.181
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Giorgi Maisuradze, Dan Horea Lutas, Andrei Lutas, Volodymyr Pikhur, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida, Moritz Lipp, Michael Schwarz, and Daniel Gruss discovered that memory previously stored in microarchitectural fill buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12130)
Brandon Falk, Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that memory previously stored in microarchitectural load ports of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12127)
Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Marina Minkin, Daniel Moghimi, Moritz Lipp, Michael Schwarz, Jo Van Bulck, Daniel Genkin, Daniel Gruss, Berk Sunar, Frank Piessens, and Yuval Yarom discovered that memory previously stored in microarchitectural store buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2018-12126)

. . . continues on next page . . .

... continued from previous page ...

Ke Sun, Henrique Kawakami, Kekai Hu, Rodrigo Branco, Volodrmyr Pikhur, Moritz Lipp, Michael Schwarz, Daniel Gruss, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Pietro Frigo, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida discovered that uncacheable memory previously stored in microarchitectural buffers of an Intel CPU core may be exposed to a malicious process that is executing on the same CPU core. A local attacker could use this to expose sensitive information. (CVE-2019-11091)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3983-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3983.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3983-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/MDS
cve: CVE-2018-12126
cve: CVE-2018-12127
cve: CVE-2018-12130
cve: CVE-2019-11091
advisory_id: USN-3983-1
cert-bund: WID-SEC-2023-1692
cert-bund: CB-K19/0414
dfn-cert: DFN-CERT-2020-1041
dfn-cert: DFN-CERT-2020-0069
dfn-cert: DFN-CERT-2020-0048
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-2214
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1767
dfn-cert: DFN-CERT-2019-1414
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1200
dfn-cert: DFN-CERT-2019-1172
dfn-cert: DFN-CERT-2019-1151
dfn-cert: DFN-CERT-2019-1149
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-1036
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1025
dfn-cert: DFN-CERT-2019-1024
dfn-cert: DFN-CERT-2019-1017
dfn-cert: DFN-CERT-2019-1012
dfn-cert: DFN-CERT-2019-1009
dfn-cert: DFN-CERT-2019-1005
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1004
dfn-cert: DFN-CERT-2019-1003
dfn-cert: DFN-CERT-2019-1002
dfn-cert: DFN-CERT-2019-0994
dfn-cert: DFN-CERT-2019-0990
dfn-cert: DFN-CERT-2019-0989
dfn-cert: DFN-CERT-2019-0988
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0986
dfn-cert: DFN-CERT-2019-0977
dfn-cert: DFN-CERT-2019-0974
dfn-cert: DFN-CERT-2019-0971
dfn-cert: DFN-CERT-2019-0969
dfn-cert: DFN-CERT-2019-0950
dfn-cert: DFN-CERT-2018-2399
```

Medium (CVSS: 5.6)
NVT: Ubuntu: Security Advisory (USN-3524-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3524-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.139.148
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Jann Horn discovered that microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized memory reads via sidechannel attacks. This flaw is known as Meltdown. A local attacker could use this to expose sensitive information, including kernel memory.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3524-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3524.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-3524-1
cve: CVE-2017-5754
advisory_id: USN-3524-1
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-1228
cert-bund: CB-K20/0324
cert-bund: CB-K18/1140
cert-bund: CB-K18/0898
cert-bund: CB-K18/0654
cert-bund: CB-K18/0651
cert-bund: CB-K18/0557
cert-bund: CB-K18/0472
cert-bund: CB-K18/0463
cert-bund: CB-K18/0398
cert-bund: CB-K18/0381
cert-bund: CB-K18/0370
cert-bund: CB-K18/0348
cert-bund: CB-K18/0346
cert-bund: CB-K18/0283
cert-bund: CB-K18/0257
cert-bund: CB-K18/0244
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0177
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0148
cert-bund: CB-K18/0054
cert-bund: CB-K18/0051
cert-bund: CB-K18/0049
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
cert-bund: CB-K18/0022
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0010
cert-bund: CB-K17/2117
cert-bund: CB-K17/2113
dfn-cert: DFN-CERT-2023-0507
dfn-cert: DFN-CERT-2018-2465
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-1794
dfn-cert: DFN-CERT-2018-1734
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0878
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0808
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0605
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0499
dfn-cert: DFN-CERT-2018-0427
dfn-cert: DFN-CERT-2018-0410
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0377
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0267
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0163
dfn-cert: DFN-CERT-2018-0066
dfn-cert: DFN-CERT-2018-0058
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2017-2211
dfn-cert: DFN-CERT-2017-2210
```

Medium (CVSS: 5.6)
NVT: Ubuntu: Security Advisory (USN-3542-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux' package(s) announced via the USN-3542-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.141.151
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

Jann Horn discovered that microprocessors utilizing speculative execution and branch prediction may allow unauthorized memory reads via sidechannel attacks. This flaw is known as Spectre. A local attacker could use this to expose sensitive information, including kernel memory. This update provides mitigations for the i386 (CVE-2017-5753 only) and amd64 architectures.

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-3542-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2018.3542.1

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3542-1
url: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown
cve: CVE-2017-5715
cve: CVE-2017-5753
advisory_id: USN-3542-1
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-1228
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K19/0774
cert-bund: CB-K18/0651
cert-bund: CB-K18/0635
cert-bund: CB-K18/0601
cert-bund: CB-K18/0551
cert-bund: CB-K18/0518
cert-bund: CB-K18/0472
cert-bund: CB-K18/0370
cert-bund: CB-K18/0367
cert-bund: CB-K18/0356
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0347
cert-bund: CB-K18/0346
cert-bund: CB-K18/0338
cert-bund: CB-K18/0283
cert-bund: CB-K18/0257
cert-bund: CB-K18/0250
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0177
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0129
cert-bund: CB-K18/0099
cert-bund: CB-K18/0094
cert-bund: CB-K18/0049
cert-bund: CB-K18/0046
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
cert-bund: CB-K18/0022
cert-bund: CB-K18/0021
cert-bund: CB-K18/0020
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0010
cert-bund: CB-K18/0009
dfn-cert: DFN-CERT-2023-1568
dfn-cert: DFN-CERT-2023-1377
dfn-cert: DFN-CERT-2023-1164
dfn-cert: DFN-CERT-2023-0879
dfn-cert: DFN-CERT-2023-0877
dfn-cert: DFN-CERT-2023-0876
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-2022-0531
dfn-cert: DFN-CERT-2021-2537
dfn-cert: DFN-CERT-2021-1829
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-1987
dfn-cert: DFN-CERT-2019-1985
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1150
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0613
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1819
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1726
dfn-cert: DFN-CERT-2018-1550
dfn-cert: DFN-CERT-2018-1504
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1386
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1108
dfn-cert: DFN-CERT-2018-1032
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0796
dfn-cert: DFN-CERT-2018-0794
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0728
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0625
dfn-cert: DFN-CERT-2018-0598
dfn-cert: DFN-CERT-2018-0552
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0382
dfn-cert: DFN-CERT-2018-0375
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0367
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0137
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0053
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0029
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0022
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2018-0019
```

Medium (CVSS: 5.6)
NVT: Ubuntu: Security Advisory (USN-3594-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3594-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.143.153
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

USN-3542-1 mitigated CVE-2017-5715 (Spectre Variant 2) for the amd64 architecture in Ubuntu 14.04 LTS. This update provides the compiler-based retpoline kernel mitigation for the amd64 and i386 architectures. Original advisory details:
Jann Horn discovered that microprocessors utilizing speculative execution and branch prediction may allow unauthorized memory reads via sidechannel attacks. This flaw is known as Spectre. A local attacker could use this to expose sensitive information, including kernel memory. (CVE-2017-5715)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3594-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2018.3594.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3594-1
url: https://usn.ubuntu.com/3542-1/
cve: CVE-2017-5715
advisory_id: USN-3594-1
cert-bund: WID-SEC-2023-0103
cert-bund: WID-SEC-2022-0532
cert-bund: CB-K19/0774
cert-bund: CB-K18/0651
cert-bund: CB-K18/0635
cert-bund: CB-K18/0551
cert-bund: CB-K18/0518
cert-bund: CB-K18/0472
cert-bund: CB-K18/0370
cert-bund: CB-K18/0367
cert-bund: CB-K18/0356
cert-bund: CB-K18/0347
cert-bund: CB-K18/0346
cert-bund: CB-K18/0338
cert-bund: CB-K18/0283
cert-bund: CB-K18/0250
cert-bund: CB-K18/0207
cert-bund: CB-K18/0184
cert-bund: CB-K18/0177
cert-bund: CB-K18/0165
cert-bund: CB-K18/0153
cert-bund: CB-K18/0099
cert-bund: CB-K18/0094
cert-bund: CB-K18/0049
cert-bund: CB-K18/0046
cert-bund: CB-K18/0040
cert-bund: CB-K18/0039
cert-bund: CB-K18/0023
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K18/0022
cert-bund: CB-K18/0021
cert-bund: CB-K18/0020
cert-bund: CB-K18/0017
cert-bund: CB-K18/0016
cert-bund: CB-K18/0010
cert-bund: CB-K18/0009
dfn-cert: DFN-CERT-2022-0531
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2019-2374
dfn-cert: DFN-CERT-2019-1837
dfn-cert: DFN-CERT-2019-1415
dfn-cert: DFN-CERT-2019-1150
dfn-cert: DFN-CERT-2018-2539
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1819
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1726
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-2018-1386
dfn-cert: DFN-CERT-2018-1385
dfn-cert: DFN-CERT-2018-1364
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1108
dfn-cert: DFN-CERT-2018-1032
dfn-cert: DFN-CERT-2018-1008
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0988
dfn-cert: DFN-CERT-2018-0933
dfn-cert: DFN-CERT-2018-0931
dfn-cert: DFN-CERT-2018-0857
dfn-cert: DFN-CERT-2018-0821
dfn-cert: DFN-CERT-2018-0819
dfn-cert: DFN-CERT-2018-0818
dfn-cert: DFN-CERT-2018-0815
dfn-cert: DFN-CERT-2018-0799
dfn-cert: DFN-CERT-2018-0796
dfn-cert: DFN-CERT-2018-0794
dfn-cert: DFN-CERT-2018-0760
dfn-cert: DFN-CERT-2018-0682
dfn-cert: DFN-CERT-2018-0663
dfn-cert: DFN-CERT-2018-0631
dfn-cert: DFN-CERT-2018-0625
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-0598
dfn-cert: DFN-CERT-2018-0552
dfn-cert: DFN-CERT-2018-0510
dfn-cert: DFN-CERT-2018-0397
dfn-cert: DFN-CERT-2018-0394
dfn-cert: DFN-CERT-2018-0382
dfn-cert: DFN-CERT-2018-0375
dfn-cert: DFN-CERT-2018-0372
dfn-cert: DFN-CERT-2018-0367
dfn-cert: DFN-CERT-2018-0310
dfn-cert: DFN-CERT-2018-0276
dfn-cert: DFN-CERT-2018-0262
dfn-cert: DFN-CERT-2018-0224
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2018-0194
dfn-cert: DFN-CERT-2018-0181
dfn-cert: DFN-CERT-2018-0167
dfn-cert: DFN-CERT-2018-0104
dfn-cert: DFN-CERT-2018-0096
dfn-cert: DFN-CERT-2018-0054
dfn-cert: DFN-CERT-2018-0053
dfn-cert: DFN-CERT-2018-0045
dfn-cert: DFN-CERT-2018-0044
dfn-cert: DFN-CERT-2018-0031
dfn-cert: DFN-CERT-2018-0030
dfn-cert: DFN-CERT-2018-0029
dfn-cert: DFN-CERT-2018-0025
dfn-cert: DFN-CERT-2018-0024
dfn-cert: DFN-CERT-2018-0022
dfn-cert: DFN-CERT-2018-0020
dfn-cert: DFN-CERT-2018-0019
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-4398-2)

Summary
The remote host is missing an update for the 'dbus' package(s) announced via the USN-4398-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libdbus-1-3
Installed version:    libdbus-1-3-1.6.18-0ubuntu4.4
Fixed version:      >=libdbus-1-3-1.6.18-0ubuntu4.5+esm2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'dbus' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4398-1 fixed a vulnerability in DBus. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Kevin Backhouse discovered that DBus incorrectly handled file descriptors. A local 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-4398-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4398.2
Version used: `2022-09-13T14:14:11Z`

References
```
url: https://ubuntu.com/security/notices/USN-4398-2
cve: CVE-2020-12049
advisory_id: USN-4398-2
cert-bund: WID-SEC-2022-2006
cert-bund: CB-K20/1049
cert-bund: CB-K20/0538
dfn-cert: DFN-CERT-2021-1569
dfn-cert: DFN-CERT-2020-2550
dfn-cert: DFN-CERT-2020-1831
dfn-cert: DFN-CERT-2020-1514
dfn-cert: DFN-CERT-2020-1162
```

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.

Vulnerability Detection Result
```
Vulnerable package:   libflac8
Installed version:    libflac8-1.3.0-2ubuntu0.14.04.1
Fixed version:      >=libflac8-1.3.0-2ubuntu0.14.04.1+esm1
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2022-11-22T04:11:06Z`

References
```
url: https://ubuntu.com/security/notices/USN-5733-1
cve: CVE-2017-6888
cve: CVE-2020-0499
cve: CVE-2021-0561
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2018-2435
dfn-cert: DFN-CERT-2018-0820
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5189-1)

Summary
The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-5189-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.40.2-0ubuntu1.1
Fixed version:      >=libglib2.0-0-2.40.2-0ubuntu1.1+esm4
Vulnerable package:   libglib2.0-data
Installed version:    libglib2.0-data-2.40.2-0ubuntu1.1
Fixed version:      >=libglib2.0-data-2.40.2-0ubuntu1.1+esm4
```

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

Affected Software/OS
'glib2.0' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
It was discovered that GLib incorrectly handled certain environment variables. An attacker could possibly 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-5189-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5189.1
Version used: `2023-04-12T04:08:59Z`

References

```
url: https://ubuntu.com/security/notices/USN-5189-1
cve: CVE-2021-3800
advisory_id: USN-5189-1
cert-bund: WID-SEC-2022-1902
dfn-cert: DFN-CERT-2021-2596
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2367
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5133-1)

Summary
The remote host is missing an update for the 'icu' package(s) announced via the USN-5133-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libicu52
Installed version:    libicu52-52.1-3ubuntu0.8
Fixed version:      >=libicu52-52.1-3ubuntu0.8+esm2
```

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

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

Vulnerability Insight
It was discovered that ICU contains a use after free issue. An attacker could use this issue to cause a denial of service with crafted input.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5133-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5133.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5133-1
cve: CVE-2020-21913
advisory_id: USN-5133-1
cert-bund: WID-SEC-2022-1330
dfn-cert: DFN-CERT-2021-2566
dfn-cert: DFN-CERT-2021-2117
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5604-1)

Summary
The remote host is missing an update for the 'tiff' package(s) announced via the USN-5604-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm3
```

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

Affected Software/OS
'tiff' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that LibTIFF incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2022-2867, CVE-2022-2869)
It was discovered that LibTIFF incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2022-2868)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5604-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5604.1
Version used: `2022-12-01T04:11:08Z`

References
```
url: https://ubuntu.com/security/notices/USN-5604-1
cve: CVE-2022-2867
cve: CVE-2022-2868
cve: CVE-2022-2869
advisory_id: USN-5604-1
cert-bund: WID-SEC-2023-0561
cert-bund: WID-SEC-2022-1061
dfn-cert: DFN-CERT-2023-0218
dfn-cert: DFN-CERT-2023-0141
dfn-cert: DFN-CERT-2023-0084
dfn-cert: DFN-CERT-2022-2601
dfn-cert: DFN-CERT-2022-2493
dfn-cert: DFN-CERT-2022-2351
dfn-cert: DFN-CERT-2022-1991
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   libtiff5
Installed version:    libtiff5-4.0.3-7ubuntu0.11
Fixed version:      >=libtiff5-4.0.3-7ubuntu0.11+esm7
```

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

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

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

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

References

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-5008-2)

Summary
The remote host is missing an update for the 'avahi' package(s) announced via the USN-5008-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   avahi-daemon
Installed version:    avahi-daemon-0.6.31-4ubuntu1.3
Fixed version:      >=avahi-daemon-0.6.31-4ubuntu1.3+esm1
Vulnerable package:   libavahi-core7
Installed version:    libavahi-core7-0.6.31-4ubuntu1.3
Fixed version:      >=libavahi-core7-0.6.31-4ubuntu1.3+esm1
```

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

Affected Software/OS
'avahi' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5008-1 fixed a vulnerability in avahi. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5008-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5008.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5008-2
cve: CVE-2021-3468
advisory_id: USN-5008-2
cert-bund: WID-SEC-2022-0143
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K21/0608
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-5690-1)

Summary
The remote host is missing an update for the 'libxdmcp' package(s) announced via the USN-5690-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libxdmcp6
Installed version:    libxdmcp6-1:1.1.1-1
Fixed version:      >=libxdmcp6-1:1.1.1-1ubuntu0.1~esm1
```

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

Affected Software/OS
'libxdmcp' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
It was discovered that libXdmcp was generating weak session keys. A local attacker could possibly use this issue to perform a brute force attack and obtain another user's key.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5690-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5690.1
Version used: `2022-10-20T04:36:45Z`

References

```
url: https://ubuntu.com/security/notices/USN-5690-1
cve: CVE-2017-2625
advisory_id: USN-5690-1
cert-bund: WID-SEC-2022-1793
cert-bund: CB-K17/1296
cert-bund: CB-K17/0360
dfn-cert: DFN-CERT-2019-2490
dfn-cert: DFN-CERT-2017-1346
dfn-cert: DFN-CERT-2017-0363
```

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.

Vulnerability Detection Result

```
Vulnerable package:   tar
Installed version:    tar-1.27.1-1ubuntu0.1
Fixed version:      >=tar-1.27.1-1ubuntu0.1+esm3
```

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 22.10.

Vulnerability Insight
It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or cause a crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5900-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5900.1
Version used: `2023-06-01T04:10:00Z`

References

```
url: https://ubuntu.com/security/notices/USN-5900-1
cve: CVE-2022-48303
advisory_id: USN-5900-1
cert-bund: WID-SEC-2023-1542
cert-bund: WID-SEC-2023-0213
dfn-cert: DFN-CERT-2023-1230
dfn-cert: DFN-CERT-2023-0404
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-4359-2)

Summary
The remote host is missing an update for the 'apt' package(s) announced via the USN-4359-2 advisory.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   apt
Installed version:    apt-1.0.1ubuntu2.19
Fixed version:      >=apt-1.0.1ubuntu2.24+esm1
```

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

Affected Software/OS
'apt' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4359-1 fixed a vulnerability in APT. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM.
Original advisory details:
It was discovered that APT incorrectly handled certain filenames during package installation. If an attacker could provide a specially crafted package to be installed by the system administrator, this could cause APT to crash.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4359-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4359.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4359-2
cve: CVE-2020-3810
advisory_id: USN-4359-2
cert-bund: CB-K20/0466
dfn-cert: DFN-CERT-2020-1166
dfn-cert: DFN-CERT-2020-1035
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-3160-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3160-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.106.114
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
CAI Qian discovered that shared bind mounts in a mount namespace exponentially added entries without restriction to the Linux kernel's mount table. A local attacker could use this to cause a denial of service (system crash). (CVE-2016-6213)
It was discovered that a race condition existed in the procfs environ_read function in the Linux kernel, leading to an integer underflow. A local attacker could use this to expose sensitive information (kernel memory). (CVE-2016-7916)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-3160-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2016.3160.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3160-1
cve: CVE-2016-6213
cve: CVE-2016-7916
advisory_id: USN-3160-1
cert-bund: CB-K18/0184
cert-bund: CB-K17/1404
cert-bund: CB-K17/1286
cert-bund: CB-K17/0697
cert-bund: CB-K17/0297
cert-bund: CB-K17/0238
cert-bund: CB-K17/0168
cert-bund: CB-K16/1999
cert-bund: CB-K16/1997
cert-bund: CB-K16/1911
cert-bund: CB-K16/1740
cert-bund: CB-K16/1739
dfn-cert: DFN-CERT-2018-0200
dfn-cert: DFN-CERT-2017-1467
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0719
dfn-cert: DFN-CERT-2017-0305
dfn-cert: DFN-CERT-2017-0249
dfn-cert: DFN-CERT-2017-0171
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-2107
dfn-cert: DFN-CERT-2016-2026
dfn-cert: DFN-CERT-2016-1844
dfn-cert: DFN-CERT-2016-1843
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-3264-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3264-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.117.127
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

Vulnerability Insight
Alexander Popov discovered that a race condition existed in the Stream Control Transmission Protocol (SCTP) implementation in the Linux kernel. A local attacker could 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-3264-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3264.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3264-1
cve: CVE-2017-5986
advisory_id: USN-3264-1
cert-bund: CB-K17/1584
cert-bund: CB-K17/1484
cert-bund: CB-K17/1267
cert-bund: CB-K17/0884
cert-bund: CB-K17/0866
cert-bund: CB-K17/0840
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K17/0838
cert-bund: CB-K17/0834
cert-bund: CB-K17/0826
cert-bund: CB-K17/0812
cert-bund: CB-K17/0690
cert-bund: CB-K17/0648
cert-bund: CB-K17/0546
cert-bund: CB-K17/0403
cert-bund: CB-K17/0401
cert-bund: CB-K17/0354
cert-bund: CB-K17/0325
dfn-cert: DFN-CERT-2017-1653
dfn-cert: DFN-CERT-2017-1551
dfn-cert: DFN-CERT-2017-1317
dfn-cert: DFN-CERT-2017-0912
dfn-cert: DFN-CERT-2017-0893
dfn-cert: DFN-CERT-2017-0866
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0861
dfn-cert: DFN-CERT-2017-0853
dfn-cert: DFN-CERT-2017-0838
dfn-cert: DFN-CERT-2017-0789
dfn-cert: DFN-CERT-2017-0713
dfn-cert: DFN-CERT-2017-0666
dfn-cert: DFN-CERT-2017-0565
dfn-cert: DFN-CERT-2017-0410
dfn-cert: DFN-CERT-2017-0408
dfn-cert: DFN-CERT-2017-0359
dfn-cert: DFN-CERT-2017-0327
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-3290-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-3290-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.119.129
```

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 14.04.

Vulnerability Insight

Marco Grassi discovered that the TCP implementation in the Linux kernel mishandles socket buffer (skb) truncation. A local attacker could 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-3290-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2017.3290.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3290-1
cve: CVE-2016-8645
advisory_id: USN-3290-1
cert-bund: CB-K17/1520
cert-bund: CB-K17/1286
cert-bund: CB-K17/0838
cert-bund: CB-K17/0836
cert-bund: CB-K17/0552
cert-bund: CB-K17/0277
cert-bund: CB-K17/0268
cert-bund: CB-K17/0260
cert-bund: CB-K17/0259
cert-bund: CB-K17/0212
cert-bund: CB-K17/0088
cert-bund: CB-K16/1999
cert-bund: CB-K16/1783
dfn-cert: DFN-CERT-2017-1583
dfn-cert: DFN-CERT-2017-1343
dfn-cert: DFN-CERT-2017-0864
dfn-cert: DFN-CERT-2017-0863
dfn-cert: DFN-CERT-2017-0564
dfn-cert: DFN-CERT-2017-0283
dfn-cert: DFN-CERT-2017-0273
dfn-cert: DFN-CERT-2017-0265
dfn-cert: DFN-CERT-2017-0264
dfn-cert: DFN-CERT-2017-0218
dfn-cert: DFN-CERT-2017-0092
dfn-cert: DFN-CERT-2016-2111
dfn-cert: DFN-CERT-2016-1886
```

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.

Vulnerability Detection Result

```
Vulnerable package:   tar
Installed version:    tar-1.27.1-1ubuntu0.1
Fixed version:      >=tar-1.27.1-1ubuntu0.1+esm2
```

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.
Details: `Ubuntu: Security Advisory (USN-5329-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5329.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5329-1
cve: CVE-2021-20193
advisory_id: USN-5329-1
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-4627-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'linux, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gke-4.15, linux-gke-5.3, linux-hwe, linux-hwe-5.4, linux-lts-trusty, linux-lts-xenial, linux-oem, linux-oem-osp1, linux-oracle, linux-oracle-5.4' package(s) announced via the USN-4627-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.183.192
```

Solution:

Solution type: VendorFix

Please install the updated package(s).

Affected Software/OS

'linux, linux-gcp, linux-gcp-4.15, linux-gcp-5.4, linux-gke-4.15, linux-gke-5.3, linux-hwe, linux-hwe-5.4, linux-lts-trusty, linux-lts-xenial, linux-oem, linux-oem-osp1, linux-oracle, linux-oracle-5.4' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight

Moritz Lipp, Michael Schwarz, Andreas Kogler, David Oswald, Catherine Easdon, Claudio Canella, and Daniel Gruss discovered that the Intel Running Average Power Limit (RAPL) driver in the Linux kernel did not properly restrict access to power data. A local attacker could possibly use this to expose sensitive information.

Vulnerability Detection Method

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

Details: `Ubuntu: Security Advisory (USN-4627-1)`

OID:1.3.6.1.4.1.25623.1.1.12.2020.4627.1

Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4627-1
cve: CVE-2020-8694
advisory_id: USN-4627-1
cert-bund: WID-SEC-2022-0999
cert-bund: CB-K20/1093
dfn-cert: DFN-CERT-2021-2185
dfn-cert: DFN-CERT-2021-0262
dfn-cert: DFN-CERT-2020-2772
dfn-cert: DFN-CERT-2020-2731
dfn-cert: DFN-CERT-2020-2730
dfn-cert: DFN-CERT-2020-2696
dfn-cert: DFN-CERT-2020-2678
dfn-cert: DFN-CERT-2020-2676
dfn-cert: DFN-CERT-2020-2665
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2612
dfn-cert: DFN-CERT-2020-2602
dfn-cert: DFN-CERT-2020-2598
dfn-cert: DFN-CERT-2020-2597
dfn-cert: DFN-CERT-2020-2594
dfn-cert: DFN-CERT-2020-2592
dfn-cert: DFN-CERT-2020-2579
dfn-cert: DFN-CERT-2020-2522
dfn-cert: DFN-CERT-2020-2509
dfn-cert: DFN-CERT-2020-2496
dfn-cert: DFN-CERT-2020-2489
dfn-cert: DFN-CERT-2020-2488
dfn-cert: DFN-CERT-2020-2487
dfn-cert: DFN-CERT-2020-2476
dfn-cert: DFN-CERT-2020-2475
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-5916-1)

Summary
The remote host is missing an update for the 'linux' package(s) announced via the USN-5916-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.192.202
```

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

Affected Software/OS
'linux' package(s) on Ubuntu 14.04.

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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5916-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.5916.1

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2023-03-06T04:11:16Z

References

```
url: https://ubuntu.com/security/notices/USN-5916-1
cve: CVE-2022-42703
advisory_id: USN-5916-1
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1669
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-1651
dfn-cert: DFN-CERT-2023-1592
dfn-cert: DFN-CERT-2023-1542
dfn-cert: DFN-CERT-2023-1253
dfn-cert: DFN-CERT-2023-1116
dfn-cert: DFN-CERT-2023-1041
dfn-cert: DFN-CERT-2023-0508
dfn-cert: DFN-CERT-2022-2915
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-2022-2818
dfn-cert: DFN-CERT-2022-2817
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-2022-2609
dfn-cert: DFN-CERT-2022-2599
dfn-cert: DFN-CERT-2022-2543
dfn-cert: DFN-CERT-2022-2520
```

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.

Vulnerability Detection Result

```
Vulnerable package:   unzip
Installed version:    unzip-6.0-9ubuntu1.5
Fixed version:      >=unzip-6.0-9ubuntu1.6+esm1
```

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)

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: `2022-12-01T04:11:08Z`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-4503-1)

Summary
The remote host is missing an update for the 'libdbi-perl' package(s) announced via the USN-4503-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libdbi-perl
Installed version:    libdbi-perl-1.630-1
Fixed version:      >=libdbi-perl-1.630-1ubuntu0.1~esm1
```

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

Affected Software/OS
'libdbi-perl' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
It was discovered that Perl DBI module incorrectly handled certain calls. 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-4503-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4503.1
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4503-1
cve: CVE-2020-14392
advisory_id: USN-4503-1
dfn-cert: DFN-CERT-2020-2011
```

Medium (CVSS: 5.5)
NVT: Ubuntu: Security Advisory (USN-4451-2)

Summary
The remote host is missing an update for the 'ppp' package(s) announced via the USN-4451-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ppp
Installed version:    ppp-2.4.5-5.1ubuntu2.3
Fixed version:      >=ppp-2.4.5-5.1ubuntu2.3+esm2
```

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

Affected Software/OS
'ppp' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4451-1 fixed a vulnerability in ppp. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Thomas Chauchefoin working with Trend Micro's Zero Day Initiative, discovered that ppp incorrectly handled module loading. A local attacker could use this issue to load arbitrary kernel modules 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-4451-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4451.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4451-2
cve: CVE-2020-15704
advisory_id: USN-4451-2
dfn-cert: DFN-CERT-2020-1702
```

Medium (CVSS: 5.4)
NVT: Ubuntu: Security Advisory (USN-4217-2)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-4217-2 advisory.

... continues on next page ...

. . . continued from previous page . . .

Vulnerability Detection Result

```
Vulnerable package:   libsmbclient
Installed version:    libsmbclient-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=libsmbclient-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm4
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm4
```

Solution:

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

Affected Software/OS

'samba' package(s) on Ubuntu 14.04.

Vulnerability Insight

USN-4217-1 fixed several vulnerabilities in Samba. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:
Andreas Oster discovered that the Samba DNS management server incorrectly handled certain records. An authenticated attacker could possibly use this issue to crash Samba, resulting in a denial of service. (CVE-2019-14861)
Isaac Boukris discovered that Samba did not enforce the Kerberos DelegationNotAllowed feature restriction, contrary to expectations. (CVE-2019-14870)

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4217-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4217.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4217-2
cve: CVE-2019-14861
cve: CVE-2019-14870
advisory_id: USN-4217-2
cert-bund: WID-SEC-2022-2051
cert-bund: CB-K19/1048
dfn-cert: DFN-CERT-2022-2612
dfn-cert: DFN-CERT-2022-2603
dfn-cert: DFN-CERT-2021-1167
dfn-cert: DFN-CERT-2020-2026
dfn-cert: DFN-CERT-2019-2593
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-4221-1)

Summary
The remote host is missing an update for the 'libpcap' package(s) announced via the USN-4221-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libpcap0.8
Installed version:    libpcap0.8-1.5.3-2
Fixed version:      >=libpcap0.8-1.5.3-2ubuntu0.1
```

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

Affected Software/OS
'libpcap' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 19.04.

Vulnerability Insight
It was discovered that libpcap did not properly validate PHB headers in some situations. An attacker could use this to cause a denial of service (memory exhaustion).

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4221-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4221.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4221-1
cve: CVE-2019-15165
advisory_id: USN-4221-1
cert-bund: WID-SEC-2022-0193
cert-bund: CB-K20/1076
cert-bund: CB-K19/1065
dfn-cert: DFN-CERT-2019-2621
dfn-cert: DFN-CERT-2019-2196
dfn-cert: DFN-CERT-2019-2153
dfn-cert: DFN-CERT-2019-2128
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-4903-1)

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

The remote host is missing an update for the 'curl' package(s) announced via the USN-4903-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm7
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm7
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm7
```

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

Affected Software/OS
'curl' package(s) on Ubuntu 14.04.

Vulnerability Insight
Viktor Szakats discovered that curl did not strip off user credentials from referrer header fields. 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-4903-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4903.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4903-1
cve: CVE-2021-22876
advisory_id: USN-4903-1
cert-bund: WID-SEC-2023-1634
cert-bund: WID-SEC-2023-1350
cert-bund: CB-K22/0044
cert-bund: CB-K21/0333
dfn-cert: DFN-CERT-2022-0835
dfn-cert: DFN-CERT-2022-0076
dfn-cert: DFN-CERT-2021-2527
dfn-cert: DFN-CERT-2021-2369
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2021-1329
dfn-cert: DFN-CERT-2021-1174
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2021-1165
dfn-cert: DFN-CERT-2021-0807
dfn-cert: DFN-CERT-2021-0701
dfn-cert: DFN-CERT-2021-0663
dfn-cert: DFN-CERT-2021-0653
```

Medium (CVSS: 5.3)
NVT: Ubuntu: Security Advisory (USN-4455-1)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4455-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm7
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04.

Vulnerability Insight
It was discovered that NSS incorrectly handled certain signatures. An attacker could possibly use this issue to expose sensitive information. (CVE-2020-12400, CVE-2020-12401, CVE-2020-6829)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4455-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4455.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4455-1
cve: CVE-2020-12400
cve: CVE-2020-12401
cve: CVE-2020-6829
advisory_id: USN-4455-1
cert-bund: WID-SEC-2022-1831
cert-bund: CB-K20/1030
cert-bund: CB-K20/0842
dfn-cert: DFN-CERT-2023-0411
dfn-cert: DFN-CERT-2021-0715
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2137
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1918
dfn-cert: DFN-CERT-2020-1852
dfn-cert: DFN-CERT-2020-1646
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-4049-4)

Summary
The remote host is missing an update for the 'glib2.0' package(s) announced via the USN-4049-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libglib2.0-0
Installed version:    libglib2.0-0-2.40.2-0ubuntu1.1
Fixed version:      >=libglib2.0-0-2.40.2-0ubuntu1.1+esm3
```

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

Affected Software/OS
'glib2.0' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4049-1 fixed a vulnerability in GLib. The update introduced a regression. This update fixes the problem.
We apologize for the inconvenience.
Original advisory details:
It was discovered that GLib created directories and files without properly restricting permissions. An attacker could possibly use this issue to access sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4049-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4049.4
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4049-4
url: https://launchpad.net/bugs/1838890
advisory_id: USN-4049-4
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-6105-2)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-6105-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20170717~14.04.2
Fixed version:      >=ca-certificates-20230311~14.04.1~esm1
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-6105-1 updated ca-certificates. This provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-6105-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6105.2
Version used: `2023-05-25T04:09:16Z`

References

```
url: https://ubuntu.com/security/notices/USN-6105-2
url: https://launchpad.net/bugs/
advisory_id: USN-6105-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5761-2)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5761-2 advisory.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20170717~14.04.2
Fixed version:      >=ca-certificates-20211016~14.04.1~esm1
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5761-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5761-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5761.2
Version used: `2022-12-07T04:10:10Z`

References
```
url: https://ubuntu.com/security/notices/USN-5761-2
url: https://launchpad.net/bugs/XXXXXX
advisory_id: USN-5761-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5089-2)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-5089-2 advisory.

Vulnerability Detection Result
```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20170717~14.04.2
Fixed version:      >=ca-certificates-20190110~14.04.1~esm2
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5089-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5089-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5089.2
Version used: `2022-08-26T07:43:23Z`

References
```
url: https://ubuntu.com/security/notices/USN-5089-2
url: https://launchpad.net/bugs/1944481
advisory_id: USN-5089-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-3976-4)

Summary
The remote host is missing an update for the 'samba' package(s) announced via the USN-3976-4 advisory.

Vulnerability Detection Result
```
Vulnerable package:   samba
Installed version:    samba-2:4.3.11+dfsg-0ubuntu0.14.04.20
Fixed version:      >=samba-2:4.3.11+dfsg-0ubuntu0.14.04.20+esm2
```

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

Affected Software/OS
'samba' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-3976-1 fixed a vulnerability in Samba. The update introduced a regression causing Samba to occasionally crash. This update fixes the problem.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

Isaac Boukris and Andrew Bartlett discovered that Samba incorrectly checked S4U2Self packets. In certain environments, a remote attacker could possibly 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-3976-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.3976.4
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-3976-4
url: https://launchpad.net/bugs/1827924
advisory_id: USN-3976-4
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-4377-2)

Summary
The remote host is missing an update for the 'ca-certificates' package(s) announced via the USN-4377-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   ca-certificates
Installed version:    ca-certificates-20170717~14.04.2
Fixed version:      >=ca-certificates-20190110~14.04.1~esm1
```

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

Affected Software/OS
'ca-certificates' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4377-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
The ca-certificates package contained an expired CA certificate that caused connectivity issues. This update removes the 'AddTrust External Root' CA.
In addition, on Ubuntu 12.04 ESM and Ubuntu 14.04 ESM, this update refreshes the included certificates to those contained in the 20190110 package.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4377-2)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.1.12.2020.4377.2
Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4377-2
url: https://launchpad.net/bugs/1881533
advisory_id: USN-4377-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-4038-4)

Summary

The remote host is missing an update for the 'bzip2' package(s) announced via the USN-4038-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   bzip2
Installed version:    bzip2-1.0.6-5
Fixed version:      >=bzip2-1.0.6-5ubuntu0.1~esm2
Vulnerable package:   libbz2-1.0
Installed version:    libbz2-1.0-1.0.6-5
Fixed version:      >=libbz2-1.0-1.0.6-5ubuntu0.1~esm2
```

Solution:

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

Affected Software/OS

'bzip2' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4038-1 fixed a vulnerability in bzip2. The update introduced a regression causing bzip2 to incorrect raises CRC errors for some files. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM.
We apologize for the inconvenience.
Original advisory details:
It was discovered that bzip2 incorrectly handled certain 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-4038-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2019.4038.4
Version used: 2022-09-13T14:14:11Z

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://ubuntu.com/security/notices/USN-4038-4
url: https://launchpad.net/bugs/1834494
advisory_id: USN-4038-4
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5588-1)

Summary

The remote host is missing an update for the 'linux' package(s) announced via the USN-5588-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.191.201
```

Solution:

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

Affected Software/OS

'linux' package(s) on Ubuntu 14.04.

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.

Vulnerability Detection Method

Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5588-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5588.1
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5588-1
cve: CVE-2022-2588
advisory_id: USN-5588-1
cert-bund: WID-SEC-2023-1737
cert-bund: WID-SEC-2023-1432
cert-bund: WID-SEC-2022-0997
dfn-cert: DFN-CERT-2023-0661
dfn-cert: DFN-CERT-2022-2915
dfn-cert: DFN-CERT-2022-2649
dfn-cert: DFN-CERT-2022-2623
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-2022-2469
dfn-cert: DFN-CERT-2022-2446
dfn-cert: DFN-CERT-2022-2423
dfn-cert: DFN-CERT-2022-2390
dfn-cert: DFN-CERT-2022-2382
dfn-cert: DFN-CERT-2022-2304
dfn-cert: DFN-CERT-2022-2300
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-2022-2112
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
dfn-cert: DFN-CERT-2022-2037
dfn-cert: DFN-CERT-2022-2034
dfn-cert: DFN-CERT-2022-1966
dfn-cert: DFN-CERT-2022-1828
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-2022-1776
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-5745-2)

Summary
The remote host is missing an update for the ’shadow’ package(s) announced via the USN-5745-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   login
Installed version:    login-1:4.1.5.1-1ubuntu9.5
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:      >=login-1:4.1.5.1-1ubuntu9.5+esm3
Vulnerable package:   passwd
Installed version:    passwd-1:4.1.5.1-1ubuntu9.5
Fixed version:      >=passwd-1:4.1.5.1-1ubuntu9.5+esm3
```

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-5060-2)

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the USN-5060-2 advisory.

Vulnerability Detection Result
```
Vulnerable package:   ntfs-3g
Installed version:    ntfs-3g-1:2013.1.13AR.1-2ubuntu2
Fixed version:      >=ntfs-3g-1:2013.1.13AR.1-2ubuntu2+esm1
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

Affected Software/OS
'ntfs-3g' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
USN-5060-1 fixed a vulnerability in NTFS-3G. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
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-5060-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.5060.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-5060-2
url: https://launchpad.net/bugs/1942235
advisory_id: USN-5060-2
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-4986-4)

Summary
The remote host is missing an update for the 'rpcbind' package(s) announced via the USN-4986-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   rpcbind
Installed version:    rpcbind-0.2.1-2ubuntu2.2
Fixed version:      >=rpcbind-0.2.1-2ubuntu2.2+esm2
```

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

Affected Software/OS
'rpcbind' package(s) on Ubuntu 14.04, Ubuntu 16.04.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

USN-4986-1 fixed a vulnerability in rpcbind. The update caused a regression resulting in rpcbind crashing in certain environments. This update fixes the problem for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.
Original advisory details:
It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind 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-4986-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4986.4
Version used: `2022-08-26T07:43:23Z`

References

```
url: https://ubuntu.com/security/notices/USN-4986-4
url: https://launchpad.net/bugs/1931507
advisory_id: USN-4986-4
```

Medium (CVSS: 5.0)
NVT: Ubuntu: Security Advisory (USN-4360-3)

Summary

The remote host is missing an update for the 'json-c' package(s) announced via the USN-4360-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libjson-c2
Installed version:    libjson-c2-0.11-3ubuntu1.2
Fixed version:      >=libjson-c2-0.11-3ubuntu1.2+esm2
Vulnerable package:   libjson0
Installed version:    libjson0-0.11-3ubuntu1.2
Fixed version:      >=libjson0-0.11-3ubuntu1.2+esm2
```

Solution:

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

Affected Software/OS

'json-c' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight

USN-4360-1 fixed a vulnerability in json-c. The security fix introduced a memory leak in some scenarios. This update reverts the security fix pending further investigation.
We apologize for the inconvenience.

. . . continues on next page . . .

. . . continued from previous page . . .

Original advisory details:
It was discovered that json-c incorrectly handled certain JSON 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-4360-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4360.3
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4360-3
url: https://launchpad.net/bugs/1878723
advisory_id: USN-4360-3
```

Medium (CVSS: 4.7)
NVT: Ubuntu: Security Advisory (USN-4534-1)

Summary
The remote host is missing an update for the 'libdbi-perl' package(s) announced via the USN-4534-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libdbi-perl
Installed version:    libdbi-perl-1.630-1
Fixed version:      >=libdbi-perl-1.630-1ubuntu0.1~esm5
```

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

Affected Software/OS
'libdbi-perl' package(s) on Ubuntu 12.04, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Vulnerability Insight
It was discovered that Perl DBI module incorrectly handled certain inputs. An attacker could possibly use this issue to cause a 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-4534-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4534.1
Version used: `2022-08-26T07:43:23Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-4534-1
cve: CVE-2019-20919
advisory_id: USN-4534-1
dfn-cert: DFN-CERT-2021-0002
dfn-cert: DFN-CERT-2020-2176
dfn-cert: DFN-CERT-2020-2172
dfn-cert: DFN-CERT-2020-2067
dfn-cert: DFN-CERT-2020-2011
```

Medium (CVSS: 4.7)
NVT: Ubuntu: Security Advisory (USN-4247-3)

Summary
The remote host is missing an update for the 'python-apt' package(s) announced via the USN-4247-3 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python-apt
Installed version:    python-apt-0.9.3.5
Fixed version:      >=python-apt-0.9.3.5ubuntu3+esm2
Vulnerable package:   python3-apt
Installed version:    python3-apt-0.9.3.5
Fixed version:      >=python3-apt-0.9.3.5ubuntu3+esm2
```

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

Affected Software/OS
'python-apt' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4247-1 fixed several vulnerabilities in python-apt. This update provides the corresponding updates for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a machine-in-the-middle attack, this flaw could potentially be used to install altered packages. (CVE-2019-15795)
It was discovered that python-apt could install packages from untrusted repositories, contrary to expectations. (CVE-2019-15796)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4247-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4247.3

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: 2022-09-13T14:14:11Z

References

```
url: https://ubuntu.com/security/notices/USN-4247-3
cve: CVE-2019-15795
cve: CVE-2019-15796
advisory_id: USN-4247-3
dfn-cert: DFN-CERT-2020-0308
dfn-cert: DFN-CERT-2020-0166
```

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.

Vulnerability Detection Result

```
Vulnerable package:   login
Installed version:    login-1:4.1.5.1-1ubuntu9.5
Fixed version:      >=login-1:4.1.5.1-1ubuntu9.5+esm2
Vulnerable package:   passwd
Installed version:    passwd-1:4.1.5.1-1ubuntu9.5
Fixed version:      >=passwd-1:4.1.5.1-1ubuntu9.5+esm2
```

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: 2022-11-29T04:10:49Z

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: 4.7)
NVT: Ubuntu: Security Advisory (USN-5737-1)

Summary
The remote host is missing an update for the 'apr-util' package(s) announced via the USN-5737-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libaprutil1
Installed version:    libaprutil1-1.5.3-1
Fixed version:      >=libaprutil1-1.5.3-1ubuntu0.1~esm1
```

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

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

Vulnerability Insight
It was discovered that APR-util did not properly handle memory when using SDBM database files. A local attacker with write access to the database can make a program or process using these functions crash, and 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-5737-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5737.1
Version used: `2022-11-24T04:10:36Z`

References

```
url: https://ubuntu.com/security/notices/USN-5737-1
cve: CVE-2017-12618
advisory_id: USN-5737-1
cert-bund: WID-SEC-2023-1594
cert-bund: WID-SEC-2022-2156
cert-bund: CB-K19/0612
cert-bund: CB-K18/1050
cert-bund: CB-K17/2175
cert-bund: CB-K17/2021
cert-bund: CB-K17/1834
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2019-1457
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2017-2270
dfn-cert: DFN-CERT-2017-2108
dfn-cert: DFN-CERT-2017-1911
```

Medium (CVSS: 4.4)
NVT: Ubuntu: Security Advisory (USN-4417-2)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4417-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm6
```

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

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4417-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Cesar Pereida, Billy Bob Brumley, Yuval Yarom, and Nicola Tuveri discovered that NSS incorrectly handled RSA key generation. A local attacker could possibly use this issue to perform a timing attack and recover RSA keys.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4417-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4417.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4417-2
cve: CVE-2020-12402
advisory_id: USN-4417-2
cert-bund: WID-SEC-2023-0457
cert-bund: CB-K20/1030
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K20/0650
dfn-cert: DFN-CERT-2021-0715
dfn-cert: DFN-CERT-2020-2299
dfn-cert: DFN-CERT-2020-2191
dfn-cert: DFN-CERT-2020-2137
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1697
dfn-cert: DFN-CERT-2020-1566
dfn-cert: DFN-CERT-2020-1562
dfn-cert: DFN-CERT-2020-1560
dfn-cert: DFN-CERT-2020-1450
dfn-cert: DFN-CERT-2020-1437
dfn-cert: DFN-CERT-2020-1404
dfn-cert: DFN-CERT-2020-1391
```

Medium (CVSS: 4.4)
NVT: Ubuntu: Security Advisory (USN-5211-1)

Summary
The remote host is missing an update for the 'linux, linux-aws, linux-kvm, linux-lts-xenial' package(s) announced via the USN-5211-1 advisory.

Vulnerability Detection Result

```
Vulnerable package:   linux-image-generic
Installed version:    linux-image-generic-3.13.0.24.28
Fixed version:      >=linux-image-generic-3.13.0.189.198
```

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

Affected Software/OS
'linux, linux-aws, linux-kvm, linux-lts-xenial' package(s) on Ubuntu 14.04, Ubuntu 16.04.

Vulnerability Insight
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.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-5211-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2022.5211.1
Version used: `2022-09-13T14:14:11Z`

References

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://ubuntu.com/security/notices/USN-5211-1
cve: CVE-2021-4002
advisory_id: USN-5211-1
cert-bund: WID-SEC-2022-0515
cert-bund: WID-SEC-2022-0230
cert-bund: CB-K21/1238
dfn-cert: DFN-CERT-2022-1453
dfn-cert: DFN-CERT-2022-1294
dfn-cert: DFN-CERT-2022-1057
dfn-cert: DFN-CERT-2022-0983
dfn-cert: DFN-CERT-2022-0920
dfn-cert: DFN-CERT-2022-0557
dfn-cert: DFN-CERT-2022-0548
dfn-cert: DFN-CERT-2022-0547
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-2022-0196
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-2022-0026
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-2021-2480
```

Medium (CVSS: 4.4)
NVT: Ubuntu: Security Advisory (USN-4397-2)

Summary
The remote host is missing an update for the 'nss' package(s) announced via the USN-4397-2 advisory.

Vulnerability Detection Result

```
Vulnerable package:   libnss3
Installed version:    libnss3-2:3.28.4-0ubuntu0.14.04.5
Fixed version:      >=libnss3-2:3.28.4-0ubuntu0.14.04.5+esm5
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
'nss' package(s) on Ubuntu 12.04, Ubuntu 14.04.

Vulnerability Insight
USN-4397-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM.
Original advisory details:
Cesar Pereida Garcia discovered that NSS incorrectly handled DSA key generation. A local attacker could possibly use this issue to perform a timing attack and recover DSA keys. (CVE-2020-12399)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-4397-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2020.4397.2
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4397-2
cve: CVE-2020-12399
advisory_id: USN-4397-2
cert-bund: CB-K20/0541
cert-bund: CB-K20/0525
dfn-cert: DFN-CERT-2020-2110
dfn-cert: DFN-CERT-2020-1566
dfn-cert: DFN-CERT-2020-1533
dfn-cert: DFN-CERT-2020-1450
dfn-cert: DFN-CERT-2020-1437
dfn-cert: DFN-CERT-2020-1391
dfn-cert: DFN-CERT-2020-1316
dfn-cert: DFN-CERT-2020-1288
dfn-cert: DFN-CERT-2020-1186
dfn-cert: DFN-CERT-2020-1166
dfn-cert: DFN-CERT-2020-1157
```

[return to 10.0.0.10]

2.1.10 Medium 631/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: `2021-07-19T08:11:48Z`

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 10.0.0.10]

2.1.11 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

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

Vulnerability Detection Result

```
The remote SSH server supports the following weak host key algorithm(s):
host key algorithm | Description
-------------------------------------------------------------------------------
↪---------
ssh-dss            | Digital Signature Algorithm (DSA) / Digital Signature Stand
↪ard (DSS)
```

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

Vulnerability Detection Method
Checks the supported host key algorithms of the remote SSH server.
Currently weak host key algorithms are defined as the following:
- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Details: `Weak Host Key Algorithm(s) (SSH)`
OID:1.3.6.1.4.1.25623.1.0.117687
Version used: `2021-11-24T06:31:19Z`

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

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

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                          | Reason
-------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.

A nation-state can break a 1024-bit prime.

Vulnerability Detection Method

Checks the supported KEX algorithms of the remote SSH server.

Currently weak KEX algorithms are defined as the following:

- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key

Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.150713

Version used: `2022-12-08T10:12:32Z`

References

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142.html
url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple
↪m
url: https://datatracker.ietf.org/doc/html/rfc6194
```

Medium (CVSS: 4.3)

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

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

Vulnerability Insight

- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

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

Currently weak encryption algorithms are defined as the following:

- Arcfour (RC4) cipher based algorithms

. . . continues on next page . . .

. . . continued from previous page . . .

- none algorithm
- CBC mode cipher based algorithms

Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2022-12-09T10:11:04Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3
url: https://www.kb.cert.org/vuls/id/958563
```

[return to 10.0.0.10]

2.1.12 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Anonymous login ok, send your complete email address
↪ as your password
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-07-14T16:09:27Z`

[return to 10.0.0.10]

2.1.13 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.

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: 23991585
Packet 2: 23991852
```

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-05-11T09:09:33Z`

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

[return to 10.0.0.10]

2.1.14 Low package

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.

Vulnerability Detection Result

```
Vulnerable package:   curl
Installed version:    curl-7.35.0-1ubuntu2.20
Fixed version:      >=curl-7.35.0-1ubuntu2.20+esm12
Vulnerable package:   libcurl3
Installed version:    libcurl3-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-7.35.0-1ubuntu2.20+esm12
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.35.0-1ubuntu2.20
Fixed version:      >=libcurl3-gnutls-7.35.0-1ubuntu2.20+esm12
```

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
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: `2022-10-03T04:28:47Z`

References

```
url: https://ubuntu.com/security/notices/USN-5587-1
cve: CVE-2022-35252
advisory_id: USN-5587-1
cert-bund: WID-SEC-2023-1728
cert-bund: WID-SEC-2023-1614
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-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: 2.8)
NVT: Ubuntu: Security Advisory (USN-4668-4)

Summary
The remote host is missing an update for the 'python-apt' package(s) announced via the USN-4668-4 advisory.

Vulnerability Detection Result

```
Vulnerable package:   python-apt
Installed version:    python-apt-0.9.3.5
Fixed version:      >=python-apt-0.9.3.5ubuntu3+esm4
Vulnerable package:   python3-apt
Installed version:    python3-apt-0.9.3.5
Fixed version:      >=python3-apt-0.9.3.5ubuntu3+esm4
```

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

Affected Software/OS
'python-apt' package(s) on Ubuntu 14.04.

Vulnerability Insight
USN-4668-1 fixed a vulnerability in python-apt. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

. . . continues on next page . . .

. . . continued from previous page . . .

Kevin Backhouse discovered that python-apt incorrectly handled resources. A local attacker could possibly use this issue to cause python-apt 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-4668-4)`
OID:1.3.6.1.4.1.25623.1.1.12.2021.4668.4
Version used: `2022-09-13T14:14:11Z`

References

```
url: https://ubuntu.com/security/notices/USN-4668-4
cve: CVE-2020-27351
advisory_id: USN-4668-4
dfn-cert: DFN-CERT-2020-2690
```

[return to 10.0.0.10]

2.1.15 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

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

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

Solution:
Solution type: Mitigation

. . . continues on next page . . .

. . . continued from previous page . . .

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

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

Currently weak MAC algorithms are defined as the following:

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

Details: `Weak MAC Algorithm(s) Supported (SSH)`

OID:1.3.6.1.4.1.25623.1.0.105610

Version used: `2021-09-20T11:05:40Z`

[return to 10.0.0.10]

2.1.16 Low general/icmp

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

Summary

The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result

```
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

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

Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

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

[return to 10.0.0.10]

This file was automatically generated.