tenable Nessus

Report generated by Tenable Nessus™

DC - 5

Sat, 08 Nov 2025 18:50:46 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.50.41.35

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	32	55	7	73

Scan Information

Start time:	Sat Nov 8 18:44:03 2025
End time:	Sat Nov 8 18:50:46 2025

Host Information

IP:	10.50.41.35
MAC Address:	08:00:27:23:F7:DA
OS:	Linux Kernel 3.16.0-4-amd64 on Debian 8.10

Vulnerabilities

128556 - Debian DLA-1911-1 : exim4 security update -

Synopsis

The remote Debian host is missing a security update.

Description

'Zerons' and Qualys discovered that a buffer overflow triggerable in the TLS negotiation code of the Exim mail transport agent could result in the execution of arbitrary code with root privileges.

For Debian 8 'Jessie', this problem has been fixed in version 4.84.2-2+deb8u6.

We recommend that you upgrade your exim4 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/2019/09/msg00004.html
https://packages.debian.org/source/jessie/exim4

Solution

Upgrade the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-15846

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : exim4_4.84.2-2+deb8u5
Should be : exim4_4.84.2-2+deb8u6
Remote package installed : exim4-base_4.84.2-2+deb8u5
Should be : exim4-base_4.84.2-2+deb8u6
Remote package installed : exim4-config_4.84.2-2+deb8u5
Should be : exim4-config_4.84.2-2+deb8u6
Remote package installed : exim4-daemon-light_4.84.2-2+deb8u5
Should be : exim4-daemon-light_4.84.2-2+deb8u6
```

129361 - Debian DLA-1930-1 : 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-2016-10905

A race condition was discovered in the GFS2 file-system implementation, which could lead to a use-after-free. On a system using GFS2, a local attacker could use this for denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2018-20976

It was discovered that the XFS file-system implementation did not correctly handle some mount failure conditions, which could lead to a use-after-free. The security impact of this is unclear.

CVE-2018-21008

It was discovered that the rsi wifi driver did not correctly handle some failure conditions, which could lead to a use-after- free. The security impact of this is unclear.

CVE-2019-0136

It was discovered that the wifi soft-MAC implementation (mac80211) did not properly authenticate Tunneled Direct Link Setup (TDLS) messages.
A nearby attacker could use this for denial of service (loss of wifi connectivity).

CVE-2019-9506

Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen discovered a weakness in the Bluetooth pairing protocols, dubbed the 'KNOB attack'. An attacker that is nearby during pairing could use this to weaken the encryption used between the paired devices, and then to eavesdrop on and/or spoof communication between them.

This update mitigates the attack by requiring a minimum encryption key length of 56 bits.

CVE-2019-14814, CVE-2019-14815, CVE-2019-14816

Multiple bugs were discovered in the mwifiex wifi driver, which could lead to heap buffer overflows. A local user permitted to configure a device handled by this driver could probably use this for privilege escalation.

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.

CVE-2019-15211

The syzkaller tool found a bug in the radio-raremono driver that could lead to a use-after-free. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-15212

The syzkaller tool found that the rio500 driver does not work correctly if more than one device is bound to it. 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.

CVE-2019-15215

The syzkaller tool found a bug in the cpia2_usb driver that leads to a use-after-free. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-15218

The syzkaller tool found that the smsusb driver did not validate that USB devices have the expected endpoints, potentially leading to a NULL pointer dereference. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops).

CVE-2019-15219

The syzkaller tool found that a device initialisation error in the sisusbvga driver could lead to a NULL pointer dereference. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops).

CVE-2019-15220

The syzkaller tool found a race condition in the p54usb driver which could lead to a use-after-free. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-15221

The syzkaller tool found that the line6 driver did not validate USB devices' maximum packet sizes, which could lead to a heap buffer overrun. 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.

CVE-2019-15292

The Hulk Robot tool found missing error checks in the Appletalk protocol implementation, which could lead to a use-after-free. The security impact of this is unclear.

CVE-2019-15807

Jian Luo reported that the Serial Attached SCSI library (libsas) did not correctly handle failure to discover devices beyond a SAS expander. This could lead to a resource leak and crash (BUG). The security impact of this is unclear.

CVE-2019-15917

The syzkaller tool found a race condition in code supporting UART-attached Bluetooth adapters, which could lead to a use- after-free. A local user with access to a pty device or other suitable tty device could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-15926

It was found that the ath6kl wifi driver did not consistently validate traffic class numbers in received control packets, leading to out-of-bounds memory accesses. A nearby attacker on the same wifi network could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.74-1.

We recommend that you upgrade your linux 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/2019/09/msg00025.html
https://packages.debian.org/source/jessie/linux

Solution

Upgrade the affected packages.

Risk Factor

Critical

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

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2016-10905
CVE	CVE-2018-20976
CVE	CVE-2018-21008
CVE	CVE-2019-0136
CVE	CVE-2019-14814
CVE	CVE-2019-14815
CVE	CVE-2019-14816
CVE	CVE-2019-14821
CVE	CVE-2019-14835
CVE	CVE-2019-15117
CVE	CVE-2019-15118
CVE	CVE-2019-15211
CVE	CVE-2019-15212
CVE	CVE-2019-15215
CVE	CVE-2019-15218
CVE	CVE-2019-15219
CVE	CVE-2019-15220
CVE	CVE-2019-15221
CVE	CVE-2019-15292
CVE	CVE-2019-15807
CVE	CVE-2019-15917

CVE	CVE-2019-15926
CVE	CVE-2019-9506

Plugin Information

Published: 2019/09/26, Modified: 2024/04/23

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.74-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.74-1

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.
```

133101 - Debian DLA-2068-1 : 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 leak.

CVE-2019-2215

The syzkaller tool discovered a use-after-free vulnerability in the Android binder driver. A local user on a system with this driver enabled could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation. However, this driver is not enabled on Debian packaged kernels.

CVE-2019-10220

Various developers and researchers found that if a crafted file- system or malicious file server presented a directory with filenames including a '/' character, this could confuse and possibly defeat security checks in applications that read the directory.

The kernel will now return an error when reading such a directory, rather than passing the invalid filenames on to user-space.

CVE-2019-14895, CVE-2019-14901

ADLab of Venustech discovered potential heap buffer overflows in the mwifiex wifi driver. On systems using this driver, a malicious Wireless Access Point or adhoc/P2P peer could use these to cause a denial of service (memory corruption or crash) or possibly for remote code execution.

CVE-2019-14896, CVE-2019-14897

ADLab of Venustech discovered potential heap and stack buffer overflows in the libertas wifi driver. On systems using this driver, a malicious Wireless Access Point or adhoc/P2P peer could use these to cause a denial of service (memory corruption or crash) or possibly for remote code execution.

CVE-2019-15098

Hui Peng and Mathias Payer reported that the ath6kl wifi driver did not properly validate USB descriptors, which could lead to a NULL pointer derefernce. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops).

CVE-2019-15217

The syzkaller tool discovered that the zr364xx mdia driver did not correctly handle devices without a product name string, which could lead to a NULL pointer dereference. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops).

CVE-2019-15291

The syzkaller tool discovered that the b2c2-flexcop-usb media driver did not properly validate USB descriptors, which could lead to a NULL pointer dereference. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops).

CVE-2019-15505

The syzkaller tool discovered that the technisat-usb2 media driver did not properly validate incoming IR packets, which could lead to a heap buffer over-read. An attacker able to add USB devices could use this to cause a denial of service (BUG/oops) or to read sensitive information from kernel memory.

CVE-2019-16746

It was discovered that the wifi stack did not validate the content of beacon heads provided by user-space for use on a wifi interface in Access Point mode, which could lead to a heap buffer overflow. A local user permitted to configure a wifi interface could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056

Ori Nimron reported that various network protocol implementations

- AX.25, IEEE 802.15.4, Appletalk, ISDN, and NFC - allowed all users to create raw sockets. A local user could use this to send arbitrary packets on networks using those protocols.

CVE-2019-17133

Nicholas Waisman reported that the wifi stack did not valdiate received SSID information before copying it, which could lead to a buffer overflow if it is not validated by the driver or firmware. A malicious Wireless Access Point might be able to use this to cause a denial of service (memory corruption or crash) or for remote code execution.

CVE-2019-17666

Nicholas Waisman reported that the rtlwifi wifi drivers did not properly validate received P2P information, leading to a buffer overflow. A malicious P2P peer could use this to cause a denial of service (memory corruption or crash) or for remote code execution.

CVE-2019-19051

Navid Emamdoost discovered a potential memory leak in the i2400m wimax driver if the software rfkill operation fails. The security impact of this is unclear.

CVE-2019-19052

Navid Emamdoost discovered a potential memory leak in the gs_usb CAN driver if the open (interface-up) operation fails. The security impact of this is unclear.

CVE-2019-19056, CVE-2019-19057

Navid Emamdoost discovered potential memory leaks in the mwifiex wifi driver if the probe operation fails. The security impact of this is unclear.

CVE-2019-19062

Navid Emamdoost discovered a potential memory leak in the AF_ALG subsystem if the CRYPTO_MSG_GETALG operation fails. A local user could possibly use this to cause a denial of service (memory exhaustion).

CVE-2019-19066

Navid Emamdoost discovered a potential memory leak in the bfa SCSI driver if the get_fc_host_stats operation fails. The security impact of this is unclear.

CVE-2019-19227

Dan Carpenter reported missing error checks in the Appletalk protocol implementation that could lead to a NULL pointer dereference. The security impact of this is unclear.

CVE-2019-19332

The syzkaller tool discovered a missing bounds check in the KVM implementation for x86, which could lead to a heap buffer overflow. A local user permitted to use KVM could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19523

The syzkaller tool discovered a use-after-free bug in the adutux USB driver. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19524

The syzkaller tool discovered a race condition in the ff-memless library used by input drivers. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19527

The syzkaller tool discovered that the hiddev driver did not correctly handle races between a task opening the device and disconnection of the underlying hardware. A local user permitted to access hiddev devices, and able to add and remove USB devices, could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19530

The syzkaller tool discovered a potential use-after-free in the cdc-acm network driver. 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.

CVE-2019-19531

The syzkaller tool discovered a use-after-free bug in the yurex USB driver. An attacker able to add and remove USB devices could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19532

The syzkaller tool discovered a potential heap buffer overflow in the hid-gaff input driver, which was also found to exist in many other input drivers. 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.

CVE-2019-19533

The syzkaller tool discovered that the ttusb-dec media driver was missing initialisation of a structure, which could leak sensitive information from kernel memory.

CVE-2019-19534, CVE-2019-19536

The syzkaller tool discovered that the peak_usb CAN driver was missing initialisation of some structures, which could leak sensitive information from kernel memory.

CVE-2019-19537

The syzkaller tool discovered race conditions in the USB stack, involving character device registration. 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.

CVE-2019-19767

The syzkaller tool discovered that crafted ext4 volumes could trigger a buffer overflow in the ext4 filesystem driver. An attacker able to mount such a volume could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-19922

It was discovered that a change in Linux 3.16.61, 'sched/fair: Fix bandwidth timer clock drift condition', could lead to tasks being throttled before using their full quota of CPU time. A local user could use this bug to slow down other users' tasks. This change has been reverted.

CVE-2019-19947

It was discovered that the kvaser_usb CAN driver was missing initialisation of some structures, which could leak sensitive information from kernel memory.

CVE-2019-19965

Gao Chuan reported a race condition in the libsas library used by SCSI host drivers, which could lead to a NULL pointer dereference. An attacker able to add and remove SCSI devices could use this to cause a denial of service (BUG/oops).

CVE-2019-19966

The syzkaller tool discovered a missing error check in the cpia2 media driver, which could lead to a use-after-free. 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.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.81-1.

We recommend that you upgrade your linux 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/2020/01/msg00013.html
https://packages.debian.org/source/jessie/linux

Solution

Upgrade the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-10220
CVE	CVE-2019-14895
CVE	CVE-2019-14896
CVE	CVE-2019-14897
CVE	CVE-2019-14901
CVE	CVE-2019-15098
CVE	CVE-2019-15217
CVE	CVE-2019-15291
CVE	CVE-2019-15505
CVE	CVE-2019-16746
CVE	CVE-2019-17052
CVE	CVE-2019-17053
CVE	CVE-2019-17054
CVE	CVE-2019-17055
CVE	CVE-2019-17056
CVE	CVE-2019-17133
CVE	CVE-2019-17666
CVE	CVE-2019-19051
CVE	CVE-2019-19052
CVE	CVE-2019-19056
CVE	CVE-2019-19057
CVE	CVE-2019-19062
CVE	CVE-2019-19066
CVE	CVE-2019-19227
CVE	CVE-2019-19332
CVE	CVE-2019-19523
CVE	CVE-2019-19524
CVE	CVE-2019-19527
CVE	CVE-2019-19530
CVE	CVE-2019-19531
CVE	CVE-2019-19532
CVE	CVE-2019-19533
CVE	CVE-2019-19534
CVE	CVE-2019-19536
CVE	CVE-2019-19537
CVE	CVE-2019-19767
CVE	CVE-2019-19922
CVE	CVE-2019-19947
CVE	CVE-2019-19965
CVE	CVE-2019-19966
CVE	CVE-2019-2215
XREF	CISA-KNOWN-EXPLOITED:2022/05/03

Exploitable With

Metasploit (true)

Plugin Information

Published: 2020/01/21, Modified: 2024/03/29

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.81-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.81-1

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.
```

109517 - Debian DSA-4187-1 : linux - security update (Spectre)

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-2015-9016 Ming Lei reported a race condition in the multiqueue block layer (blk-mq). On a system with a driver using blk-mq (mtip32xx, null_blk, or virtio_blk), a local user might be able to use this for denial of service or possibly for privilege escalation.

- CVE-2017-0861 Robb Glasser reported a potential use-after-free in the ALSA (sound) PCM core. We believe this was not possible in practice.

- CVE-2017-5715 Multiple researchers have discovered a vulnerability in various processors supporting speculative execution, enabling an attacker controlling an unprivileged process to read memory from arbitrary addresses, including from the kernel and all other processes running on the system.

This specific attack has been named Spectre variant 2 (branch target injection) and is mitigated for the x86 architecture (amd64 and i386) by using the 'retpoline' compiler feature which allows indirect branches to be isolated from speculative execution.

- CVE-2017-5753 Multiple researchers have discovered a vulnerability in various processors supporting speculative execution, enabling an attacker controlling an unprivileged process to read memory from arbitrary addresses, including from the kernel and all other processes running on the system.

This specific attack has been named Spectre variant 1 (bounds-check bypass) and is mitigated by identifying vulnerable code sections (array bounds checking followed by array access) and replacing the array access with the speculation-safe array_index_nospec() function.

More use sites will be added over time.

- CVE-2017-13166 A bug in the 32-bit compatibility layer of the v4l2 ioctl handling code has been found. Memory protections ensuring user-provided buffers always point to userland memory were disabled, allowing destination addresses to be in kernel space. On a 64-bit kernel a local user with access to a suitable video device can exploit this to overwrite kernel memory, leading to privilege escalation.

- CVE-2017-13220 Al Viro reported that the Bluetooth HIDP implementation could dereference a pointer before performing the necessary type check. A local user could use this to cause a denial of service.

- CVE-2017-16526 Andrey Konovalov reported that the UWB subsystem may dereference an invalid pointer in an error case. A local user might be able to use this for denial of service.

- CVE-2017-16911 Secunia Research reported that the USB/IP vhci_hcd driver exposed kernel heap addresses to local users.
This information could aid the exploitation of other vulnerabilities.

- CVE-2017-16912 Secunia Research reported that the USB/IP stub driver failed to perform a range check on a received packet header field, leading to an out-of-bounds read. A remote user able to connect to the USB/IP server could use this for denial of service.

- CVE-2017-16913 Secunia Research reported that the USB/IP stub driver failed to perform a range check on a received packet header field, leading to excessive memory allocation. A remote user able to connect to the USB/IP server could use this for denial of service.

- CVE-2017-16914 Secunia Research reported that the USB/IP stub driver failed to check for an invalid combination of fields in a received packet, leading to a NULL pointer dereference. A remote user able to connect to the USB/IP server could use this for denial of service.

- CVE-2017-18017 Denys Fedoryshchenko reported that the netfilter xt_TCPMSS module failed to validate TCP header lengths, potentially leading to a use-after-free. If this module is loaded, it could be used by a remote attacker for denial of service or possibly for code execution.

- CVE-2017-18203 Hou Tao reported that there was a race condition in creation and deletion of device-mapper (DM) devices. A local user could potentially use this for denial of service.

- CVE-2017-18216 Alex Chen reported that the OCFS2 filesystem failed to hold a necessary lock during nodemanager sysfs file operations, potentially leading to a NULL pointer dereference. A local user could use this for denial of service.

- CVE-2017-18232 Jason Yan reported a race condition in the SAS (Serial-Attached SCSI) subsystem, between probing and destroying a port. This could lead to a deadlock. A physically present attacker could use this to cause a denial of service.

- CVE-2017-18241 Yunlei He reported that the f2fs implementation does not properly initialise its state if the 'noflush_merge'
mount option is used. A local user with access to a filesystem mounted with this option could use this to cause a denial of service.

- CVE-2018-1066 Dan Aloni reported to Red Hat that the CIFS client implementation would dereference a NULL pointer if the server sent an invalid response during NTLMSSP setup negotiation. This could be used by a malicious server for denial of service.

- CVE-2018-1068 The syzkaller tool found that the 32-bit compatibility layer of ebtables did not sufficiently validate offset values. On a 64-bit kernel, a local user with the CAP_NET_ADMIN capability (in any user namespace) could use this to overwrite kernel memory, possibly leading to privilege escalation. Debian disables unprivileged user namespaces by default.

- CVE-2018-1092 Wen Xu reported that a crafted ext4 filesystem image would trigger a null dereference when mounted. A local user able to mount arbitrary filesystems could use this for denial of service.

- CVE-2018-5332 Mohamed Ghannam reported that the RDS protocol did not sufficiently validate RDMA requests, leading to an out-of-bounds write. A local attacker on a system with the rds module loaded could use this for denial of service or possibly for privilege escalation.

- CVE-2018-5333 Mohamed Ghannam reported that the RDS protocol did not properly handle an error case, leading to a NULL pointer dereference. A local attacker on a system with the rds module loaded could possibly use this for denial of service.

- CVE-2018-5750 Wang Qize reported that the ACPI sbshc driver logged a kernel heap address. This information could aid the exploitation of other vulnerabilities.

- CVE-2018-5803 Alexey Kodanev reported that the SCTP protocol did not range-check the length of chunks to be created. A local or remote user could use this to cause a denial of service.

- CVE-2018-6927 Li Jinyue reported that the FUTEX_REQUEUE operation on futexes did not check for negative parameter values, which might lead to a denial of service or other security impact.

- CVE-2018-7492 The syzkaller tool found that the RDS protocol was lacking a null pointer check. A local attacker on a system with the rds module loaded could use this for denial of service.

- CVE-2018-7566 Fan LongFei reported a race condition in the ALSA (sound) sequencer core, between write and ioctl operations. This could lead to an out-of-bounds access or use-after-free. A local user with access to a sequencer device could use this for denial of service or possibly for privilege escalation.

- CVE-2018-7740 Nic Losby reported that the hugetlbfs filesystem's mmap operation did not properly range-check the file offset.
A local user with access to files on a hugetlbfs filesystem could use this to cause a denial of service.

- CVE-2018-7757 Jason Yan reported a memory leak in the SAS (Serial-Attached SCSI) subsystem. A local user on a system with SAS devices could use this to cause a denial of service.

- CVE-2018-7995 Seunghun Han reported a race condition in the x86 MCE (Machine Check Exception) driver. This is unlikely to have any security impact.

- CVE-2018-8781 Eyal Itkin reported that the udl (DisplayLink) driver's mmap operation did not properly range-check the file offset. A local user with access to a udl framebuffer device could exploit this to overwrite kernel memory, leading to privilege escalation.

- CVE-2018-8822 Dr Silvio Cesare of InfoSect reported that the ncpfs client implementation did not validate reply lengths from the server. An ncpfs server could use this to cause a denial of service or remote code execution in the client.

- CVE-2018-1000004 Luo Quan reported a race condition in the ALSA (sound) sequencer core, between multiple ioctl operations. This could lead to a deadlock or use-after-free. A local user with access to a sequencer device could use this for denial of service or possibly for privilege escalation.

- CVE-2018-1000199 Andy Lutomirski discovered that the ptrace subsystem did not sufficiently validate hardware breakpoint settings.
Local users can use this to cause a denial of service, or possibly for privilege escalation, on x86 (amd64 and i386) and possibly other architectures.

See Also

https://security-tracker.debian.org/tracker/CVE-2015-9016
https://security-tracker.debian.org/tracker/CVE-2017-0861
https://security-tracker.debian.org/tracker/CVE-2017-5715
https://security-tracker.debian.org/tracker/CVE-2017-5753
https://security-tracker.debian.org/tracker/CVE-2017-13166
https://security-tracker.debian.org/tracker/CVE-2017-13220
https://security-tracker.debian.org/tracker/CVE-2017-16526
https://security-tracker.debian.org/tracker/CVE-2017-16911
https://security-tracker.debian.org/tracker/CVE-2017-16912
https://security-tracker.debian.org/tracker/CVE-2017-16913
https://security-tracker.debian.org/tracker/CVE-2017-16914
https://security-tracker.debian.org/tracker/CVE-2017-18017
https://security-tracker.debian.org/tracker/CVE-2017-18203
https://security-tracker.debian.org/tracker/CVE-2017-18216
https://security-tracker.debian.org/tracker/CVE-2017-18232
https://security-tracker.debian.org/tracker/CVE-2017-18241
https://security-tracker.debian.org/tracker/CVE-2018-1066
https://security-tracker.debian.org/tracker/CVE-2018-1068
https://security-tracker.debian.org/tracker/CVE-2018-1092
https://security-tracker.debian.org/tracker/CVE-2018-5332
https://security-tracker.debian.org/tracker/CVE-2018-5333
https://security-tracker.debian.org/tracker/CVE-2018-5750
https://security-tracker.debian.org/tracker/CVE-2018-5803
https://security-tracker.debian.org/tracker/CVE-2018-6927
https://security-tracker.debian.org/tracker/CVE-2018-7492
https://security-tracker.debian.org/tracker/CVE-2018-7566
https://security-tracker.debian.org/tracker/CVE-2018-7740
https://security-tracker.debian.org/tracker/CVE-2018-7757
https://security-tracker.debian.org/tracker/CVE-2018-7995
https://security-tracker.debian.org/tracker/CVE-2018-8781
https://security-tracker.debian.org/tracker/CVE-2018-8822
https://security-tracker.debian.org/tracker/CVE-2018-1000004
https://security-tracker.debian.org/tracker/CVE-2018-1000199
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/jessie/linux
https://www.debian.org/security/2018/dsa-4187

Solution

Upgrade the linux packages.

For the oldstable distribution (jessie), these problems have been fixed in version 3.16.56-1.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2015-9016
CVE	CVE-2017-0861
CVE	CVE-2017-13166
CVE	CVE-2017-13220
CVE	CVE-2017-16526
CVE	CVE-2017-16911
CVE	CVE-2017-16912
CVE	CVE-2017-16913
CVE	CVE-2017-16914
CVE	CVE-2017-18017
CVE	CVE-2017-18203
CVE	CVE-2017-18216
CVE	CVE-2017-18232
CVE	CVE-2017-18241
CVE	CVE-2017-5715
CVE	CVE-2017-5753
CVE	CVE-2018-1000004
CVE	CVE-2018-1000199
CVE	CVE-2018-1066
CVE	CVE-2018-1068
CVE	CVE-2018-1092
CVE	CVE-2018-5332
CVE	CVE-2018-5333
CVE	CVE-2018-5750
CVE	CVE-2018-5803
CVE	CVE-2018-6927
CVE	CVE-2018-7492
CVE	CVE-2018-7566
CVE	CVE-2018-7740
CVE	CVE-2018-7757
CVE	CVE-2018-7995
CVE	CVE-2018-8781
CVE	CVE-2018-8822
XREF	DSA:4187
XREF	IAVA:2018-A-0020

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2018/05/02, Modified: 2024/10/15

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.56-1

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.
```

201420 - Debian Linux SEoL (8.x)

Synopsis

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

Description

According to its version, Debian Linux is 8.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/2018/20180601

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 8 (jessie)
Security End of Life : June 17, 2018
Time since Security End of Life (Est.) : >= 7 years
```

111082 - Debian DLA-1422-2 : linux security update (Spectre)

Synopsis

The remote Debian host is missing a security update.

Description

The previous update to linux failed to build for the armhf (ARM EABI hard-float) architecture. This update corrects that. For all other architectures, there is no need to upgrade or reboot again. For reference, the relevant part of the original advisory text follows.

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

CVE-2017-5715

Multiple researchers have discovered a vulnerability in various processors supporting speculative execution, enabling an attacker controlling an unprivileged process to read memory from arbitrary addresses, including from the kernel and all other processes running on the system.

This specific attack has been named Spectre variant 2 (branch target injection) and is mitigated for the x86 architecture (amd64 and i386) by using new microcoded features.

This mitigation requires an update to the processor's microcode, which is non-free. For recent Intel processors, this is included in the intel-microcode package from version 3.20180425.1~deb8u1. For other processors, it may be included in an update to the system BIOS or UEFI firmware, or in a later update to the amd64-microcode package.

This vulnerability was already mitigated for the x86 architecture by the 'retpoline' feature.

CVE-2017-5753

Further instances of code that was vulnerable to Spectre variant 1 (bounds-check bypass) have been mitigated.

CVE-2018-1066

Dan Aloni reported to Red Hat that the CIFS client implementation would dereference a NULL pointer if the server sent an invalid response during NTLMSSP setup negotiation. This could be used by a malicious server for denial of service.

The previously applied mitigation for this issue was not appropriate for Linux 3.16 and has been replaced by an alternate fix.

CVE-2018-1093

Wen Xu reported that a crafted ext4 filesystem image could trigger an out-of-bounds read in the ext4_valid_block_bitmap() function. A local user able to mount arbitrary filesystems could use this for denial of service.

CVE-2018-1130

The syzbot software found that the DCCP implementation of sendmsg() does not check the socket state, potentially leading to a NULL pointer dereference. A local user could use this to cause a denial of service (crash).

CVE-2018-3665

Multiple researchers have discovered that some Intel x86 processors can speculatively read floating-point and vector registers even when access to those registers is disabled. The Linux kernel's 'lazy FPU'
feature relies on that access control to avoid saving and restoring those registers for tasks that do not use them, and was enabled by default on x86 processors that do not support the XSAVEOPT instruction.

If 'lazy FPU' is enabled on one of the affected processors, an attacker controlling an unprivileged process may be able to read sensitive information from other users' processes or the kernel. This specifically affects processors based on the 'Nehalem' and 'Westemere' core designs. This issue has been mitigated by disabling 'lazy FPU' by default on all x86 processors that support the FXSAVE and FXRSTOR instructions, which includes all processors known to be affected and most processors that perform speculative execution. It can also be mitigated by adding the kernel parameter: eagerfpu=on

CVE-2018-5814

Jakub Jirasek reported race conditions in the USB/IP host driver. A malicious client could use this to cause a denial of service (crash or memory corruption), and possibly to execute code, on a USB/IP server.

CVE-2018-9422

It was reported that the futex() system call could be used by an unprivileged user for privilege escalation.

CVE-2018-10853

Andy Lutomirski and Mika Penttilä reported that KVM for x86 processors did not perform a necessary privilege check when emulating certain instructions. This could be used by an unprivileged user in a guest VM to escalate their privileges within the guest.

CVE-2018-10940

Dan Carpenter reported that the optical disc driver (cdrom) does not correctly validate the parameter to the CDROM_MEDIA_CHANGED ioctl. A user with access to a cdrom device could use this to cause a denial of service (crash).

CVE-2018-11506

Piotr Gabriel Kosinski and Daniel Shapira reported that the SCSI optical disc driver (sr) did not allocate a sufficiently large buffer for sense data. A user with access to a SCSI optical disc device that can produce more than 64 bytes of sense data could use this to cause a denial of service (crash or memory corruption), and possibly for privilege escalation.

CVE-2018-12233

Shankara Pailoor reported that a crafted JFS filesystem image could trigger a denial of service (memory corruption). This could possibly also be used for privilege escalation.

CVE-2018-1000204

The syzbot software found that the SCSI generic driver (sg) would in some circumstances allow reading data from uninitialised buffers, which could include sensitive information from the kernel or other tasks. However, only privileged users with the CAP_SYS_ADMIN or CAP_SYS_RAWIO capability were allowed to do this, so this has little or no security impact.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.57-1. This update additionally fixes Debian bug #898165, and includes many more bug fixes from stable update 3.16.57.

We recommend that you upgrade your linux 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/2018/07/msg00016.html
https://packages.debian.org/source/jessie/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

7.5 (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-2017-5715
CVE	CVE-2017-5753
CVE	CVE-2018-1000204
CVE	CVE-2018-1066
CVE	CVE-2018-10853
CVE	CVE-2018-1093
CVE	CVE-2018-10940
CVE	CVE-2018-1130
CVE	CVE-2018-11506
CVE	CVE-2018-12233
CVE	CVE-2018-3665
CVE	CVE-2018-5814
CVE	CVE-2018-9422

Exploitable With

CANVAS (true)

Plugin Information

Published: 2018/07/16, Modified: 2024/09/04

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.57-2

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.
```

122514 - Debian DLA-1698-2 : file regression update -

Synopsis

The remote Debian host is missing a security update.

Description

This update fixes a regression in introduced in 1:5.22+15-2+deb8u5 causing truncated output of the interpreter name, thanks to Christoph Biedl for reporting the problem and cause.

For Debian 8 'Jessie', this problem has been fixed in version 1:5.22+15-2+deb8u7.

We recommend that you upgrade your file 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/2019/11/msg00037.html
https://packages.debian.org/source/jessie/file

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2019/03/01, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : file_1:5.22+15-2+deb8u5
Should be : file_1:5.22+15-2+deb8u7
Remote package installed : libmagic1_1:5.22+15-2+deb8u5
Should be : libmagic1_1:5.22+15-2+deb8u7
```

123420 - Debian DLA-1731-2 : linux regression update (Spectre) -

Synopsis

The remote Debian host is missing a security update.

Description

The linux update issued as DLA-1731-1 caused a regression in the vmxnet3 (VMware virtual network adapter) driver. This update corrects that regression, and an earlier regression in the CIFS network filesystem implementation introduced in DLA-1422-1. For reference the original advisory text follows.

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

CVE-2016-10741

A race condition was discovered in XFS that would result in a crash (BUG). A local user permitted to write to an XFS volume could use this for denial of service.

CVE-2017-5753

Further instances of code that was vulnerable to Spectre variant 1 (bounds-check bypass) have been mitigated.

CVE-2017-13305

A memory over-read was discovered in the keys subsystem's encrypted key type. A local user could use this for denial of service or possibly to read sensitive information.

CVE-2018-3639 (SSB)

Multiple researchers have discovered that Speculative Store Bypass (SSB), a feature implemented in many processors, could be used to read sensitive information from another context. In particular, code in a software sandbox may be able to read sensitive information from outside the sandbox. This issue is also known as Spectre variant 4.

This update fixes bugs in the mitigations for SSB for AMD processors.

CVE-2018-5848

The wil6210 wifi driver did not properly validate lengths in scan and connection requests, leading to a possible buffer overflow. On systems using this driver, a local user with the CAP_NET_ADMIN capability could use this for denial of service (memory corruption or crash) or potentially for privilege escalation.

CVE-2018-5953

The swiotlb subsystem printed kernel memory addresses to the system log, which could help a local attacker to exploit other vulnerabilities.

CVE-2018-12896, CVE-2018-13053

Team OWL337 reported possible integer overflows in the POSIX timer implementation. These might have some security impact.

CVE-2018-16862

Vasily Averin and Pavel Tikhomirov from Virtuozzo Kernel Team discovered that the cleancache memory management feature did not invalidate cached data for deleted files. On Xen guests using the tmem driver, local users could potentially read data from other users'
deleted files if they were able to create new files on the same volume.

CVE-2018-16884

A flaw was found in the NFS 4.1 client implementation. Mounting NFS shares in multiple network namespaces at the same time could lead to a user-after-free. Local users might be able to use this for denial of service (memory corruption or crash) or possibly for privilege escalation.

This can be mitigated by disabling unprivileged users from creating user namespaces, which is the default in Debian.

CVE-2018-17972

Jann Horn reported that the /proc/*/stack files in procfs leaked sensitive data from the kernel. These files are now only readable by users with the CAP_SYS_ADMIN capability (usually only root)

CVE-2018-18281

Jann Horn reported a race condition in the virtual memory manager that can result in a process briefly having access to memory after it is freed and reallocated. A local user permitted to create containers could possibly exploit this for denial of service (memory corruption) or for privilege escalation.

CVE-2018-18690

Kanda Motohiro reported that XFS did not correctly handle some xattr (extended attribute) writes that require changing the disk format of the xattr. A user with access to an XFS volume could use this for denial of service.

CVE-2018-18710

It was discovered that the cdrom driver does not correctly validate the parameter to the CDROM_SELECT_DISC ioctl. A user with access to a cdrom device could use this to read sensitive information from the kernel or to cause a denial of service (crash).

CVE-2018-19824

Hui Peng and Mathias Payer discovered a use-after-free bug in the USB audio driver. A physically present attacker able to attach a specially designed USB device could use this for privilege escalation.

CVE-2018-19985

Hui Peng and Mathias Payer discovered a missing bounds check in the hso USB serial driver. A physically present user able to attach a specially designed USB device could use this to read sensitive information from the kernel or to cause a denial of service (crash).

CVE-2018-20169

Hui Peng and Mathias Payer discovered missing bounds checks in the USB core. A physically present attacker able to attach a specially designed USB device could use this to cause a denial of service (crash) or possibly for privilege escalation.

CVE-2018-20511

InfoSect reported an information leak in the AppleTalk IP/DDP implemntation. A local user with CAP_NET_ADMIN capability could use this to read sensitive information from the kernel.

CVE-2019-3701

Muyu Yu and Marcus Meissner reported that the CAN gateway implementation allowed the frame length to be modified, typically resulting in out-of-bounds memory-mapped I/O writes. On a system with CAN devices present, a local user with CAP_NET_ADMIN capability in the initial net namespace could use this to cause a crash (oops) or other hardware-dependent impact.

CVE-2019-3819

A potential infinite loop was discovered in the HID debugfs interface exposed under /sys/kernel/debug/hid. A user with access to these files could use this for denial of service.

This interface is only accessible to root by default, which fully mitigates the issue.

CVE-2019-6974

Jann Horn reported a use-after-free bug in KVM. A local user with access to /dev/kvm could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-7221

Jim Mattson and Felix Wilhelm reported a user-after-free bug in KVM's nested VMX implementation. On systems with Intel CPUs, a local user with access to /dev/kvm could use this to cause a denial of service (memory corruption or crash) or possibly for privilege escalation.

Nested VMX is disabled by default, which fully mitigates the issue.

CVE-2019-7222

Felix Wilhelm reported an information leak in KVM for x86. A local user with access to /dev/kvm could use this to read sensitive information from the kernel.

CVE-2019-9213

Jann Horn reported that privileged tasks could cause stack segments, including those in other processes, to grow downward to address 0. On systems lacking SMAP (x86) or PAN (ARM), this exacerbated other vulnerabilities: a NULL pointer dereference could be exploited for privilege escalation rather than only for denial of service.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.64-1.

We recommend that you upgrade your linux 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/2019/04/msg00004.html
https://packages.debian.org/source/jessie/linux

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (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-2016-10741
CVE	CVE-2017-13305
CVE	CVE-2017-5753
CVE	CVE-2018-12896
CVE	CVE-2018-13053
CVE	CVE-2018-16862
CVE	CVE-2018-16884
CVE	CVE-2018-17972
CVE	CVE-2018-18281
CVE	CVE-2018-18690
CVE	CVE-2018-18710
CVE	CVE-2018-19824
CVE	CVE-2018-19985
CVE	CVE-2018-20169
CVE	CVE-2018-20511
CVE	CVE-2018-3639
CVE	CVE-2018-5848
CVE	CVE-2018-5953
CVE	CVE-2019-3701

CVE	CVE-2019-3819
CVE	CVE-2019-6974
CVE	CVE-2019-7221
CVE	CVE-2019-7222
CVE	CVE-2019-9213

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2019/03/28, Modified: 2024/06/07

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.64-2

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.
```

124218 - Debian DLA-1760-1 : wget security update -

Synopsis

The remote Debian host is missing a security update.

Description

Kusano Kazuhiko discovered a buffer overflow vulnerability in the handling of Internationalized Resource Identifiers (IRI) in wget, a network utility to retrieve files from the web, which could result in the execution of arbitrary code or denial of service when recursively downloading from an untrusted server.

For Debian 8 'Jessie', this problem has been fixed in version 1.16-1+deb8u6.

We recommend that you upgrade your wget 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/2019/04/msg00020.html
https://packages.debian.org/source/jessie/wget

Solution

Upgrade the affected wget package.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.5 (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-2019-5953

Plugin Information

Published: 2019/04/23, Modified: 2024/05/31

Plugin Output

tcp/0

```
Remote package installed : wget_1.16-1+deb8u5
Should be : wget_1.16-1+deb8u6
```

124282 - Debian DLA-1762-2 : systemd regression update -

Synopsis

The remote Debian host is missing a security update.

Description

In the recently uploaded systemd security update (215-17+deb8u12 via DLA-1762-1), a regression was discovered in the fix for CVE-2017-18078.

The observation of Debian jessie LTS users was, that after upgrading to

+deb8u12 temporary files would not have the correct ownerships and permissions anymore (instead of a file being owned by a specific user and/or group, files were being owned by root:root; setting POSIX file permissions (rwx, etc.) was also affected).

For Debian 8 'Jessie', this regression problem has been fixed in version 215-17+deb8u13.

We recommend that you upgrade your systemd 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/2019/04/msg00026.html
https://packages.debian.org/source/jessie/systemd

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2019/04/25, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : libsystemd0_215-17+deb8u11
Should be : libsystemd0_215-17+deb8u13
Remote package installed : libudev1_215-17+deb8u11
Should be : libudev1_215-17+deb8u13
Remote package installed : systemd_215-17+deb8u11
Should be : systemd_215-17+deb8u13
Remote package installed : systemd-sysv_215-17+deb8u11
Should be : systemd-sysv_215-17+deb8u13
Remote package installed : udev_215-17+deb8u11
Should be : udev_215-17+deb8u13
```

125478 - Debian DLA-1799-2 : linux security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) -

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.

This updated advisory text adds a note about the need to install new binary packages.

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-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091

Multiple researchers have discovered vulnerabilities in the way that Intel processor designs implement 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 across guest/host boundaries to read host memory.

See https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/m ds.html for 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) was provided via DLA-1789-1. The updated CPU microcode may also be available as part of a system firmware ('BIOS') update.

CVE-2019-2024

A use-after-free bug was discovered in the em28xx video capture driver. Local users might be able to use this for denial of service (memory corruption or crash) or possibly for privilege escalation.

CVE-2019-3459, CVE-2019-3460

Shlomi Oberman, Yuli Shapiro, and Karamba Security Ltd. research team discovered missing range checks in the Bluetooth L2CAP implementation.
If Bluetooth is enabled, a nearby attacker could use these to read sensitive information from the kernel.

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-2019-3901

Jann Horn of Google reported a race condition that would allow a local user to read performance events from a task after it executes a setuid program. This could leak sensitive information processed by setuid programs. Debian's kernel configuration does not allow unprivileged users to access peformance events by default, which fully mitigates this issue.

CVE-2019-6133

Jann Horn of Google found that Policykit's authentication check could be bypassed by a local user creating a process with the same start time and process ID as an older authenticated process. PolicyKit was already updated to fix this in DLA-1644-1. The kernel has additionally been updated to avoid a delay between assigning start time and process ID, which should make the attack impractical.

CVE-2019-9503

Hugues Anguelkov and others at Quarkslab discovered that the brcmfmac (Broadcom wifi FullMAC) driver did not correctly distinguish messages sent by the wifi firmware from other packets. An attacker using the same wifi network could use this for denial of service or to exploit other vulnerabilities in the driver.

CVE-2019-11190

Robert Święcki reported that when a setuid program was executed it was still possible to read performance events while the kernel set up the program's address space. A local user could use this to defeat ASLR in a setuid program, making it easier to exploit other vulnerabilities in the program. Debian's kernel configuration does not allow unprivileged users to access peformance events by default, which fully mitigates this issue.

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.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.68-1. This version also includes a fix for Debian bug #927781, and other fixes included in upstream stable updates.

We recommend that you upgrade your linux and linux-latest packages.
You will need to use 'apt-get upgrade --with-new-pkgs' or 'apt upgrade' as the binary package names have changed.

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/2019/05/msg00042.html
https://packages.debian.org/source/jessie/linux
https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/mds.html

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-12126
CVE	CVE-2018-12127
CVE	CVE-2018-12130
CVE	CVE-2018-5995
CVE	CVE-2019-11091
CVE	CVE-2019-11190
CVE	CVE-2019-11486
CVE	CVE-2019-11599
CVE	CVE-2019-2024
CVE	CVE-2019-3459
CVE	CVE-2019-3460
CVE	CVE-2019-3882
CVE	CVE-2019-3901
CVE	CVE-2019-6133
CVE	CVE-2019-9503
XREF	CEA-ID:CEA-2019-0547
XREF	CEA-ID:CEA-2019-0324

Plugin Information

Published: 2019/05/29, Modified: 2022/12/05

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.68-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.68-1

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.
```

125958 - Debian DLA-1823-1 : linux security update (SACK Panic) (SACK Slowness)

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-2019-3846, 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-2019-11477

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 512 unless you know that your network requires a lower value. (This value applies to Linux 3.16 only.)

CVE-2019-11810

It was discovered that the megaraid_sas driver did not correctly handle a failed memory allocation during initialisation, which could lead to a double-free. This might have some security impact, but it cannot be triggered by an unprivileged user.

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.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.68-2. Packages for PC architectures (amd64 and i386) are already available, and packages for Arm architectures (armel and armhf) will be available soon.

We recommend that you upgrade your linux 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/2019/06/msg00010.html
https://packages.debian.org/source/jessie/linux

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

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

CVSS v2.0 Temporal Score

6.5 (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-2019-11810
CVE	CVE-2019-11833
CVE	CVE-2019-11884
CVE	CVE-2019-3846
CVE	CVE-2019-5489
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-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.68-2
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.68-2

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.
```

126011 - Debian DLA-1826-1 : glib2.0 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that GLib does not properly restrict some file permissions while a copy operation is in progress; instead, default permissions are used.

For Debian 8 'Jessie', this problem has been fixed in version 2.42.1-1+deb8u1.

We recommend that you upgrade your glib2.0 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/2019/06/msg00013.html
https://packages.debian.org/source/jessie/glib2.0

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-2019-12450

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.42.1-1+b1
Should be : libglib2.0-0_2.42.1-1+deb8u1
Remote package installed : libglib2.0-data_2.42.1-1
Should be : libglib2.0-data_2.42.1-1+deb8u1
```

126348 - Debian DLA-1839-1 : expat security update -

Synopsis

The remote Debian host is missing a security update.

Description

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

For Debian 8 'Jessie', this problem has been fixed in version 2.1.0-6+deb8u5.

We recommend that you upgrade your expat 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/2019/06/msg00028.html
https://packages.debian.org/source/jessie/expat

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	CEA-ID:CEA-2021-0025

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.1.0-6+deb8u4
Should be : libexpat1_2.1.0-6+deb8u5
```

126793 - Debian DLA-1854-1 : libonig security update -

Synopsis

The remote Debian host is missing a security update.

Description

A use-after-free in onig_new_deluxe() in regext.c allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe().

For Debian 8 'Jessie', this problem has been fixed in version 5.9.5-3.2+deb8u2.

We recommend that you upgrade your libonig 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/2019/07/msg00013.html
https://packages.debian.org/source/jessie/libonig

Solution

Upgrade the affected libonig-dev, libonig2, and libonig2-dbg 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-2019-13224

Plugin Information

Published: 2019/07/19, Modified: 2024/05/09

Plugin Output

tcp/0

```
Remote package installed : libonig2_5.9.5-3.2+deb8u1
Should be : libonig2_5.9.5-3.2+deb8u2
```

126926 - Debian DLA-1860-1 : libxslt security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were found in libxslt the XSLT 1.0 processing library.

CVE-2016-4610

Invalid memory access leading to DoS at exsltDynMapFunction. libxslt allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2016-4609

Out-of-bounds read at xmlGetLineNoInternal() libxslt allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2019-13117

An xsl:number with certain format strings could lead to an uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.

CVE-2019-13118

A type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.

For Debian 8 'Jessie', these problems have been fixed in version 1.1.28-2+deb8u5.

We recommend that you upgrade your libxslt 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/2019/07/msg00020.html
https://packages.debian.org/source/jessie/libxslt

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-2016-4609
CVE	CVE-2016-4610
CVE	CVE-2019-13117
CVE	CVE-2019-13118

Plugin Information

Published: 2019/07/23, Modified: 2024/05/09

Plugin Output

tcp/0

```
Remote package installed : libxslt1.1_1.1.28-2+deb8u4
Should be : libxslt1.1_1.1.28-2+deb8u5
```

126964 - Debian DLA-1862-1 : 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-2019-2101

Andrey Konovalov discovered that the USB Video Class driver (uvcvideo) did not consistently handle a type field in device descriptors, which could result in a heap buffer overflow. This could be used for denial of service or possibly for privilege escalation.

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. In Linux 3.16 this hash function is not used for IP IDs but is used for other purposes in the network stack. In custom kernel configurations that enable kASLR, this might weaken kASLR.

CVE-2019-13272

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.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.70-1. This update also fixes a regression introduced by the original fix for CVE-2019-11478 (#930904), and includes other fixes from upstream stable updates.

We recommend that you upgrade your linux and linux-latest packages.
You will need to use 'apt-get upgrade --with-new-pkgs' or 'apt upgrade' as the binary package names have changed.

We recommend that you upgrade your linux 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/2019/07/msg00022.html
https://packages.debian.org/source/jessie/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

7.5 (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-2019-10639
CVE	CVE-2019-13272
CVE	CVE-2019-2101
XREF	CISA-KNOWN-EXPLOITED:2022/06/10

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/07/24, Modified: 2024/05/08

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.70-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.70-1

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.
```

127076 - Debian DLA-1864-1 : patch security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue with quoting has been found in patch, a tool to apply a diff file to an original, when invoking ed. In order to avoid this, ed is now directly started instead of calling a shell which starts ed.

For Debian 8 'Jessie', this problem has been fixed in version 2.7.5-1+deb8u3.

We recommend that you upgrade your patch 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/2019/07/msg00025.html
https://packages.debian.org/source/jessie/patch

Solution

Upgrade the affected patch package.

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

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-2019-13638

Plugin Information

Published: 2019/07/26, Modified: 2024/05/08

Plugin Output

tcp/0

```
Remote package installed : patch_2.7.5-1
Should be : patch_2.7.5-1+deb8u3
```

127480 - Debian DLA-1871-1 : vim security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several minor issues have been fixed in vim, a highly configurable text editor.

CVE-2017-11109

Vim allows attackers to cause a denial of service (invalid free) or possibly have unspecified other impact via a crafted source (aka -S) file.

CVE-2017-17087

Vim 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.

CVE-2019-12735

Vim did not restrict the `:source!` command when executed in a sandbox.

For Debian 8 'Jessie', these problems have been fixed in version 2:7.4.488-7+deb8u4.

We recommend that you upgrade your vim 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/2019/08/msg00003.html
https://packages.debian.org/source/jessie/vim

Solution

Upgrade the affected packages.

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-2017-11109
CVE	CVE-2017-17087
CVE	CVE-2019-12735

Plugin Information

Published: 2019/08/12, Modified: 2024/05/07

Plugin Output

tcp/0

```
Remote package installed : vim-common_2:7.4.488-7+deb8u3
Should be : vim-common_2:7.4.488-7+deb8u4
Remote package installed : vim-tiny_2:7.4.488-7+deb8u3
Should be : vim-tiny_2:7.4.488-7+deb8u4
```

127866 - Debian DLA-1884-1 : 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-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-2018-20836

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-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-2019-3900

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-2019-13631

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-2019-14283

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 ID not yet assigned)

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).

For Debian 8 'Jessie', these problems have been fixed in version 3.16.72-1.

We recommend that you upgrade your linux 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/2019/08/msg00016.html
https://packages.debian.org/source/jessie/linux

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2017-18509
CVE	CVE-2018-20836
CVE	CVE-2019-10207
CVE	CVE-2019-10638
CVE	CVE-2019-1125
CVE	CVE-2019-13631
CVE	CVE-2019-14283
CVE	CVE-2019-14284
CVE	CVE-2019-3900
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-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.72-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.72-1

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.
```

127923 - Debian DLA-1887-1 : freetype security update

Synopsis

The remote Debian host is missing a security update.

Description

A buffer over-read in the t1-parser of freetype, a font engine, has been found and fixed by checking limits more sensible.

For Debian 8 'Jessie', this problem has been fixed in version 2.5.2-3+deb8u3.

We recommend that you upgrade your freetype 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/2019/08/msg00019.html
https://packages.debian.org/source/jessie/freetype

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-2015-9290

Plugin Information

Published: 2019/08/20, Modified: 2024/05/02

Plugin Output

tcp/0

```
Remote package installed : libfreetype6_2.5.2-3+deb8u2
Should be : libfreetype6_2.5.2-3+deb8u3
```

128557 - Debian DLA-1912-1 : expat security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a heap-based buffer overread vulnerability in expat, an XML parsing library.

A specially crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer overread.

For Debian 8 'Jessie', this issue has been fixed in expat version 2.1.0-6+deb8u6.

We recommend that you upgrade your expat 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/2019/09/msg00005.html
https://packages.debian.org/source/jessie/expat

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2019/09/09, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : libexpat1_2.1.0-6+deb8u4
Should be : libexpat1_2.1.0-6+deb8u6
```

128777 - Debian DLA-1917-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a heap buffer overflow vulnerability in curl, the library and command-line tool for transferring data over the internet.

For Debian 8 'Jessie', this issue has been fixed in curl version 7.38.0-4+deb8u16.

We recommend that you upgrade your curl 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/2019/09/msg00012.html
https://packages.debian.org/source/jessie/curl

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-2019-5482

Plugin Information

Published: 2019/09/16, Modified: 2024/04/26

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.38.0-4+deb8u14
Should be : libcurl3-gnutls_7.38.0-4+deb8u16
```

129304 - Debian DLA-1928-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

An update has been made to php5, a server-side, HTML-embedded scripting language. Specficially, as reported in #805222, the ability to build extensions in certain older versions of PHP within Debian has been hindered by an upstream change which first appeared in PHP 5.6.15. This update applies a fix which restores the ability to build PHP extensions for Debian 8 'jessie' so that a forthcoming PECL extension update can be built and released.

For Debian 8 'Jessie', this problem has been fixed in version 5.6.40+dfsg-0+deb8u6.

We recommend that you upgrade your php5 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/2019/09/msg00023.html
https://packages.debian.org/source/jessie/php5

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2019/09/25, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u6
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u6
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u6
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u6
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u6
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u6
```

129766 - Debian DLA-1952-1 : rsyslog security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there were two vulnerabilities in the rsyslog system/kernel logging daemon in the parsers for AIX and Cisco log messages respectfully.

For Debian 8 'Jessie', these issue have been fixed in rsyslog version 8.4.2-1+deb8u3.

We recommend that you upgrade your rsyslog 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/2019/10/msg00011.html
https://packages.debian.org/source/jessie/rsyslog

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2019/10/10, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : rsyslog_8.4.2-1+deb8u2
Should be : rsyslog_8.4.2-1+deb8u3
```

129853 - Debian DLA-1957-1 : tzdata new upstream version -

Synopsis

The remote Debian host is missing a security update.

Description

This update includes the changes in tzdata 2018c. Notable changes are :

- Brazil has canceled DST and will stay on standard time indefinitely.

- Fiji's next DST transitions will be 2019-11-10 and 2020-01-12 instead of 2019-11-03 and 2020-01-19.

- Norfolk Island will observe Australian-style DST starting in spring 2019. The first transition is on 2019-10-06.

For Debian 8 'Jessie', this problem has been fixed in version 2019c-0+deb8u1.

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/2019/10/msg00016.html
https://packages.debian.org/source/jessie/tzdata

Solution

Upgrade the affected tzdata, and tzdata-java packages.

Risk Factor

High

Plugin Information

Published: 2019/10/15, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : tzdata_2019a-0+deb8u1
Should be : tzdata_2019c-0+deb8u1
```

130283 - Debian DLA-1970-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Emil Lerner, beched and d90pwn found a buffer underflow in php5-fpm, a Fast Process Manager for the PHP language, which can lead to remote code execution.

Instances are vulnerable depending on the web server configuration, in particular PATH_INFO handling. For a full list of preconditions, check:

https://github.com/neex/phuip-fpizdam

For Debian 8 'Jessie', this problem has been fixed in version 5.6.40+dfsg-0+deb8u7.

We recommend that you upgrade your php5 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://github.com/neex/phuip-fpizdam
https://lists.debian.org/debian-lts-announce/2019/10/msg00033.html
https://packages.debian.org/source/jessie/php5

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

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-2019-11043
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: 2019/10/28, Modified: 2024/04/16

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u7
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u7
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u7
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u7
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u7
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u7
```

131248 - Debian DLA-2003-1 : isc-dhcp security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in isc-dhcp, a server for automatic IP address assignment.

The number of simultaneous open TCP connections to OMAPI port of the server has to be limited to 200 in order to avoid a denial of service.

For Debian 8 'Jessie', this problem has been fixed in version 4.3.1-6+deb8u4.

We recommend that you upgrade your isc-dhcp 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/2019/11/msg00023.html
https://packages.debian.org/source/jessie/isc-dhcp

Solution

Upgrade the affected packages.

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2016-2774

Plugin Information

Published: 2019/11/25, Modified: 2024/04/10

Plugin Output

tcp/0

```
Remote package installed : isc-dhcp-client_4.3.1-6+deb8u3
Should be : isc-dhcp-client_4.3.1-6+deb8u4
Remote package installed : isc-dhcp-common_4.3.1-6+deb8u3
Should be : isc-dhcp-common_4.3.1-6+deb8u4
```

131705 - Debian DLA-2020-1 : libonig security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several vulnerabilities were discovered in the Oniguruma regular expressions library, notably used in PHP mbstring.

CVE-2019-19012

An integer overflow in the search_in_range function in regexec.c leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version). Remote attackers can cause a denial of service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression.

CVE-2019-19204

In the function fetch_range_quantifier in regparse.c, PFETCH is called without checking PEND. This leads to a heap-based buffer over-read and lead to denial of service via a crafted regular expression.

CVE-2019-19246

Heap-based buffer over-read in str_lower_case_match in regexec.c can lead to denial of service via a crafted regular expression.

For Debian 8 'Jessie', these problems have been fixed in version 5.9.5-3.2+deb8u4.

We recommend that you upgrade your libonig 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/2019/12/msg00002.html
https://packages.debian.org/source/jessie/libonig

Solution

Upgrade the affected libonig-dev, libonig2, and libonig2-dbg 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-2019-19012
CVE	CVE-2019-19204
CVE	CVE-2019-19246

Plugin Information

Published: 2019/12/05, Modified: 2024/04/05

Plugin Output

tcp/0

```
Remote package installed : libonig2_5.9.5-3.2+deb8u1
Should be : libonig2_5.9.5-3.2+deb8u4
```

132107 - Debian DLA-2040-1 : harfbuzz security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in harfbuzz, an OpenType text shaping engine.

Due to a buffer over-read, remote attackers are able to cause a denial of service or possibly have other impact via crafted data.

For Debian 8 'Jessie', this problem has been fixed in version 0.9.35-2+deb8u1.

We recommend that you upgrade your harfbuzz 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/2019/12/msg00022.html
https://packages.debian.org/source/jessie/harfbuzz

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.6 (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-2015-8947

Plugin Information

Published: 2019/12/18, Modified: 2024/04/04

Plugin Output

tcp/0

```
Remote package installed : libharfbuzz0b_0.9.35-2
Should be : libharfbuzz0b_0.9.35-2+deb8u1
```

132514 - Debian DLA-2052-1 : libbsd security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issues has been found in libbsd, a package containing utility functions from BSD systems.

In function fgetwln() an off-by-one error could triggers a heap buffer overflow.

For Debian 8 'Jessie', this problem has been fixed in version 0.7.0-2+deb8u1.

We recommend that you upgrade your libbsd 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/2019/12/msg00036.html
https://packages.debian.org/source/jessie/libbsd

Solution

Upgrade the affected libbsd-dev, libbsd0, and libbsd0-dbg 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-2016-2090

Plugin Information

Published: 2019/12/31, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : libbsd0_0.7.0-2
Should be : libbsd0_0.7.0-2+deb8u1
```

132681 - Debian DLA-2057-1 : pillow security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there were three vulnerabilities in Pillow, an imaging library for the Python programming language :

- CVE-2019-19911: Prevent a denial of service vulnerability caused by FpxImagePlugin.py calling the range function on an unvalidated 32-bit integer if the number of bands is large.

- CVE-2020-5312: PCX 'P mode' buffer overflow.

- CVE-2020-5313: FLI buffer overflow.

For Debian 8 'Jessie', these issues have been fixed in pillow version 2.6.1-2+deb8u4.

We recommend that you upgrade your pillow 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/2020/01/msg00003.html
https://packages.debian.org/source/jessie/pillow

Solution

Upgrade the affected packages.

Risk Factor

High

Plugin Information

Published: 2020/01/07, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : python-pil_2.6.1-2+deb8u3
Should be : python-pil_2.6.1-2+deb8u4
```

133323 - Debian DLA-2085-1 : zlib security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several issues have been found in zlib, a compression library. They are basically about improper big-endian CRC calculation, improper left shift of negative integers and improper pointer arithmetic.

For Debian 8 'Jessie', these problems have been fixed in version 1:1.2.8.dfsg-2+deb8u1.

We recommend that you upgrade your zlib 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/2020/01/msg00030.html
https://packages.debian.org/source/jessie/zlib

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-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2016-9842
CVE	CVE-2016-9843

Plugin Information

Published: 2020/01/30, Modified: 2024/03/28

Plugin Output

tcp/0

```
Remote package installed : zlib1g_1:1.2.8.dfsg-2+b1
Should be : zlib1g_1:1.2.8.dfsg-2+deb8u1
```

134352 - Debian DLA-2136-1 : libvpx security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was an out-of-bounds buffer read vulnerability in libvpx, a library implementing the VP8 & VP9 video codecs.

For Debian 8 'Jessie', this issue has been fixed in libvpx version 1.3.0-3+deb8u3.

We recommend that you upgrade your libvpx 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/2020/03/msg00009.html
https://packages.debian.org/source/jessie/libvpx

Solution

Upgrade the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-0034

Plugin Information

Published: 2020/03/10, Modified: 2024/03/25

Plugin Output

tcp/0

```
Remote package installed : libvpx1_1.3.0-3+deb8u1
Should be : libvpx1_1.3.0-3+deb8u3
```

137283 - Debian DLA-2241-2 : linux security update -

Synopsis

The remote Debian host is missing a security update.

Description

This update is now available for all supported architectures. For reference the original advisory text follows.

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

CVE-2015-8839

A race condition was found in the ext4 filesystem implementation. A local user could exploit this to cause a denial of service (filesystem corruption).

CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613

Wen Xu from SSLab at Gatech reported that crafted Btrfs volumes could trigger a crash (Oops) and/or out-of-bounds memory access. An attacker able to mount such a volume could use this to cause a denial of service or possibly for 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-2019-19447

It was discovered that the ext4 filesystem driver did not safely handle unlinking of an inode that, due to filesystem corruption, already has a link count of 0. An attacker able to mount arbitrary ext4 volumes could use this to cause a denial of service (memory corruption or 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-2019-20636

The syzbot tool found that the input subsystem did not fully validate keycode changes, which could result in a heap out-of-bounds write. A local user permitted to access the device node for an input or VT device could possibly use this to cause a denial of service (crash or memory corruption) or for privilege escalation.

CVE-2020-0009

Jann Horn reported that the Android ashmem driver did not prevent read-only files from being memory-mapped and then remapped as read-write. However, Android drivers are not enabled in Debian kernel configurations.

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-2020-1749

Xiumei Mu reported that some network protocols that can run on top of IPv6 would bypass the Transformation (XFRM) layer used by IPsec, IPcomp/IPcomp6, IPIP, and IPv6 Mobility. This could result in disclosure of information over the network, since it would not be encrypted or routed according to the system policy.

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-2020-8647, 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-2020-10690

It was discovered that the PTP hardware clock subsystem did not properly manage device lifetimes. Removing a PTP hardware clock from the system while a user process was using it could lead to a use-after-free. The security impact of this is unclear.

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-2020-10942

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-2020-12769

It was discovered that the spi-dw SPI host driver did not properly serialise access to its internal state. The security impact of this is unclear, and this driver is not included in Debian's binary packages.

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-2020-12826

Adam Zabrocki reported a weakness in the signal subsystem's permission checks. A parent process can choose an arbitary signal for a child process to send when it exits, but if the parent has executed a new program then the default SIGCHLD signal is sent. A local user permitted to run a program for several days could bypass this check, execute a setuid program, and then send an arbitrary signal to it.
Depending on the setuid programs installed, this could have some security impact.

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.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.84-1.

We recommend that you upgrade your linux 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/2020/06/msg00013.html
https://packages.debian.org/source/jessie/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-2015-8839
CVE	CVE-2018-14610
CVE	CVE-2018-14611
CVE	CVE-2018-14612
CVE	CVE-2018-14613
CVE	CVE-2019-19319
CVE	CVE-2019-19447
CVE	CVE-2019-19768
CVE	CVE-2019-20636
CVE	CVE-2019-5108
CVE	CVE-2020-0009
CVE	CVE-2020-0543
CVE	CVE-2020-10690
CVE	CVE-2020-10751
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-2020-12769
CVE	CVE-2020-12770
CVE	CVE-2020-12826
CVE	CVE-2020-13143
CVE	CVE-2020-1749
CVE	CVE-2020-2732
CVE	CVE-2020-8647
CVE	CVE-2020-8648
CVE	CVE-2020-8649
CVE	CVE-2020-9383

Plugin Information

Published: 2020/06/10, Modified: 2024/03/07

Plugin Output

tcp/0

```
  Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
  Should be : linux-image-3.16.0-<ANY>-amd64_3.16.84-1
  Remote package installed : linux-libc-dev_3.16.64-2
  Should be : linux-libc-dev_3.16.84-1

  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.
```

105704 - Debian DSA-4082-1 : linux - security update (Meltdown) -

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-2017-5754 Multiple researchers have discovered a vulnerability in Intel processors, enabling an attacker controlling an unprivileged process to read memory from arbitrary addresses, including from the kernel and all other processes running on the system.

This specific attack has been named Meltdown and is addressed in the Linux kernel for the Intel x86-64 architecture by a patch set named Kernel Page Table Isolation, enforcing a near complete separation of the kernel and userspace address maps and preventing the attack.
This solution might have a performance impact, and can be disabled at boot time by passing pti=off to the kernel command line.

- CVE-2017-8824 Mohamed Ghannam discovered that the DCCP implementation did not correctly manage resources when a socket is disconnected and reconnected, potentially leading to a use-after-free. A local user could use this for denial of service (crash or data corruption) or possibly for privilege escalation. On systems that do not already have the dccp module loaded, this can be mitigated by disabling it:echo >> /etc/modprobe.d/disable-dccp.conf install dccp false

- CVE-2017-15868 Al Viro found that the Bluebooth Network Encapsulation Protocol (BNEP) implementation did not validate the type of the second socket passed to the BNEPCONNADD ioctl(), which could lead to memory corruption. A local user with the CAP_NET_ADMIN capability can use this for denial of service (crash or data corruption) or possibly for privilege escalation.

- CVE-2017-16538 Andrey Konovalov reported that the dvb-usb-lmedm04 media driver did not correctly handle some error conditions during initialisation. A physically present user with a specially designed USB device can use this to cause a denial of service (crash).

- CVE-2017-16939 Mohamed Ghannam reported (through Beyond Security's SecuriTeam Secure Disclosure program) that the IPsec (xfrm) implementation did not correctly handle some failure cases when dumping policy information through netlink. A local user with the CAP_NET_ADMIN capability can use this for denial of service (crash or data corruption) or possibly for privilege escalation.

- CVE-2017-17448 Kevin Cernekee discovered that the netfilter subsystem allowed users with the CAP_NET_ADMIN capability in any user namespace, not just the root namespace, to enable and disable connection tracking helpers. This could lead to denial of service, violation of network security policy, or have other impact.

- CVE-2017-17449 Kevin Cernekee discovered that the netlink subsystem allowed users with the CAP_NET_ADMIN capability in any user namespace to monitor netlink traffic in all net namespaces, not just those owned by that user namespace.
This could lead to exposure of sensitive information.

- CVE-2017-17450 Kevin Cernekee discovered that the xt_osf module allowed users with the CAP_NET_ADMIN capability in any user namespace to modify the global OS fingerprint list.

- CVE-2017-17558 Andrey Konovalov reported that that USB core did not correctly handle some error conditions during initialisation. A physically present user with a specially designed USB device can use this to cause a denial of service (crash or memory corruption), or possibly for privilege escalation.

- CVE-2017-17741 Dmitry Vyukov reported that the KVM implementation for x86 would over-read data from memory when emulating an MMIO write if the kvm_mmio tracepoint was enabled. A guest virtual machine might be able to use this to cause a denial of service (crash).

- CVE-2017-17805 It was discovered that some implementations of the Salsa20 block cipher did not correctly handle zero-length input. A local user could use this to cause a denial of service (crash) or possibly have other security impact.

- CVE-2017-17806 It was discovered that the HMAC implementation could be used with an underlying hash algorithm that requires a key, which was not intended. A local user could use this to cause a denial of service (crash or memory corruption), or possibly for privilege escalation.

- CVE-2017-17807 Eric Biggers discovered that the KEYS subsystem lacked a check for write permission when adding keys to a process's default keyring. A local user could use this to cause a denial of service or to obtain sensitive information.

- CVE-2017-1000407 Andrew Honig reported that the KVM implementation for Intel processors allowed direct access to host I/O port 0x80, which is not generally safe. On some systems this allows a guest VM to cause a denial of service (crash) of the host.

- CVE-2017-1000410 Ben Seri reported that the Bluetooth subsystem did not correctly handle short EFS information elements in L2CAP messages. An attacker able to communicate over Bluetooth could use this to obtain sensitive information from the kernel.

See Also

https://security-tracker.debian.org/tracker/CVE-2017-5754
https://security-tracker.debian.org/tracker/CVE-2017-8824
https://security-tracker.debian.org/tracker/CVE-2017-15868
https://security-tracker.debian.org/tracker/CVE-2017-16538

https://security-tracker.debian.org/tracker/CVE-2017-16939
https://security-tracker.debian.org/tracker/CVE-2017-17448
https://security-tracker.debian.org/tracker/CVE-2017-17449
https://security-tracker.debian.org/tracker/CVE-2017-17450
https://security-tracker.debian.org/tracker/CVE-2017-17558
https://security-tracker.debian.org/tracker/CVE-2017-17741
https://security-tracker.debian.org/tracker/CVE-2017-17805
https://security-tracker.debian.org/tracker/CVE-2017-17806
https://security-tracker.debian.org/tracker/CVE-2017-17807
https://security-tracker.debian.org/tracker/CVE-2017-1000407
https://security-tracker.debian.org/tracker/CVE-2017-1000410
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/jessie/linux
https://www.debian.org/security/2018/dsa-4082

Solution

Upgrade the linux packages.

For the oldstable distribution (jessie), these problems have been fixed in version 3.16.51-3+deb8u1.

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-2017-1000407
CVE	CVE-2017-1000410
CVE	CVE-2017-15868
CVE	CVE-2017-16538
CVE	CVE-2017-16939
CVE	CVE-2017-17448
CVE	CVE-2017-17449
CVE	CVE-2017-17450
CVE	CVE-2017-17558
CVE	CVE-2017-17741
CVE	CVE-2017-17805
CVE	CVE-2017-17806
CVE	CVE-2017-17807
CVE	CVE-2017-5754
CVE	CVE-2017-8824
XREF	DSA:4082
XREF	IAVA:2018-A-0019

Plugin Information

Published: 2018/01/10, Modified: 2019/07/15

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.51-3+deb8u1

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.
```

109658 - Debian DSA-4196-1 : 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 or denial of service.

- CVE-2018-1087 Andy Lutomirski discovered that the KVM implementation did not properly handle #DB exceptions while deferred by MOV SS/POP SS, allowing an unprivileged KVM guest user to crash the guest or potentially escalate their privileges.

- CVE-2018-8897 Nick Peterson of Everdox Tech LLC discovered that #DB exceptions that are deferred by MOV SS or POP SS are not properly handled, allowing an unprivileged user to crash the kernel and cause a denial of service.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=897427
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=897599
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=898067
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=898100
https://security-tracker.debian.org/tracker/CVE-2018-1087
https://security-tracker.debian.org/tracker/CVE-2018-8897
https://security-tracker.debian.org/tracker/CVE-2018-1108
https://security-tracker.debian.org/tracker/source-package/linux
https://packages.debian.org/source/jessie/linux
https://packages.debian.org/source/stretch/linux
https://www.debian.org/security/2018/dsa-4196

Solution

Upgrade the linux packages.

For the oldstable distribution (jessie), these problems have been fixed in version 3.16.56-1+deb8u1. This update includes various fixes for regressions from 3.16.56-1 as released in DSA-4187-1 (Cf. #897427, #898067 and #898100).

For the stable distribution (stretch), these problems have been fixed in version 4.9.88-1+deb9u1. The fix for CVE-2018-1108 applied in DSA-4188-1 is temporarily reverted due to various regression, cf.
#897599.

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-2018-1087
CVE	CVE-2018-8897
XREF	DSA:4196

Exploitable With

Metasploit (true)

Plugin Information

Published: 2018/05/10, Modified: 2024/10/11

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
```

```
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.56-1+deb8u1

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.
```

123135 - Debian DLA-1730-4 : libssh2 regression update -

Synopsis

The remote Debian host is missing a security update.

Description

Several more boundary checks have been backported to libssh2's src/sftp.c. Furthermore, all boundary checks in src/sftp.c now result in an LIBSSH2_ERROR_BUFFER_TOO_SMALL error code, rather than a LIBSSH2_ERROR_ OUT_OF_BOUNDARY error code.

As a side note, it was discovered that libssh2's SFTP implementation from Debian jessie only works well against OpenSSH SFTP servers from Debian wheezy, tests against newer OpenSSH versions (such as available in Debian jessie and beyond) interim-fail with SFTP protocol error 'Error opening remote file'. Operation might continue after this error, this depends on application implementations.

For Debian 8 'Jessie', this problem has been fixed in version 1.4.3-4.1+deb8u5.

We recommend that you upgrade your libssh2 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/2019/07/msg00028.html
https://packages.debian.org/source/jessie/libssh2

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

7.9 (CVSS:3.0/E:U/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

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

References

CVE CVE-2019-3860

Plugin Information

Published: 2019/03/27, Modified: 2024/06/12

Plugin Output

tcp/0

```
Remote package installed : libssh2-1_1.4.3-4.1+deb8u3
Should be : libssh2-1_1.4.3-4.1+deb8u5
```

125409 - Debian DLA-1803-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A read past allocated buffer vulnerability and two heap-buffer overflow vulnerabilites were discovered in the PHP5 programming language within the Exif image module.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u3.

We recommend that you upgrade your php5 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/2019/05/msg00035.html
https://packages.debian.org/source/jessie/php5

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-2019-11034
CVE	CVE-2019-11035
CVE	CVE-2019-11036

Plugin Information

Published: 2019/05/28, Modified: 2024/05/21

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u3
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u3
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u3
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u3
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u3
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u3
```

125410 - Debian DLA-1804-1 : curl security update -

Synopsis

The remote Debian host is missing a security update.

Description

cURL, an URL transfer library, contains a heap buffer overflow in the function tftp_receive_packet() that receives data from a TFTP server.
It calls recvfrom() with the default size for the buffer rather than with the size that was used to allocate it. Thus, the content that might overwrite the heap memory is entirely controlled by the server.

For Debian 8 'Jessie', this problem has been fixed in version 7.38.0-4+deb8u15.

We recommend that you upgrade your curl 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/2019/05/msg00036.html
https://packages.debian.org/source/jessie/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-2019-5436

Plugin Information

Published: 2019/05/28, Modified: 2024/05/21

Plugin Output

tcp/0

```
Remote package installed : libcurl3-gnutls_7.38.0-4+deb8u14
Should be : libcurl3-gnutls_7.38.0-4+deb8u15
```

125682 - Debian DLA-1813-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two vulnerabilities were found in PHP, a widely-used open source general purpose scripting language.

CVE-2019-11039

An integer underflow in the iconv module could be exploited to trigger an out of bounds read.

CVE-2019-11040

A heap buffer overflow was discovered in the EXIF parsing code.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u4.

We recommend that you upgrade your php5 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/2019/06/msg00000.html
https://packages.debian.org/source/jessie/php5

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-2019-11039
CVE	CVE-2019-11040

Plugin Information

Published: 2019/06/04, Modified: 2024/05/17

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u4
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u4
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u4
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u4
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u4
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u4
```

125837 - Debian DLA-1817-1 : libgd2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

An unitialized read was discovered in the XBM support of libgd2, a library for programmatic graphics creation and manipulation. The unitialized read might lead to information disclosure.

For Debian 8 'Jessie', this problem has been fixed in version 2.1.0-5+deb8u13.

We recommend that you upgrade your libgd2 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/2019/06/msg00003.html
https://packages.debian.org/source/jessie/libgd2

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-2019-11038

Plugin Information

Published: 2019/06/12, Modified: 2024/05/16

Plugin Output

tcp/0

```
Remote package installed : libgd3_2.1.0-5+deb8u12
Should be : libgd3_2.1.0-5+deb8u13
```

126077 - Debian DLA-1828-1 : python-urllib3 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in python-urllib3, an HTTP library with thread-safe connection pooling, whereby an attacker can inject CRLF characters in the request parameter.

For Debian 8 'Jessie', this problem has been fixed in version 1.9.1-3+deb8u1.

We recommend that you upgrade your python-urllib3 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/2019/06/msg00016.html
https://packages.debian.org/source/jessie/python-urllib3

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-2019-11236

Plugin Information

Published: 2019/06/21, Modified: 2024/05/15

Plugin Output

tcp/0

```
Remote package installed : python-urllib3_1.9.1-3
Should be : python-urllib3_1.9.1-3+deb8u1
```

126222 - Debian DLA-1834-1 : python2.7 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Multiple vulnerabilities were discovered in Python, an interactive high-level object-oriented language, including

CVE-2018-14647

Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM.

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.

For Debian 8 'Jessie', these problems have been fixed in version 2.7.9-2+deb8u3.

We recommend that you upgrade your python2.7 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/2019/06/msg00022.html
https://packages.debian.org/source/jessie/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)

References

CVE	CVE-2018-14647
CVE	CVE-2019-10160
CVE	CVE-2019-5010
CVE	CVE-2019-9636
CVE	CVE-2019-9740
CVE	CVE-2019-9947
CVE	CVE-2019-9948

Plugin Information

Published: 2019/06/25, Modified: 2024/05/14

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.9-2+deb8u2
Should be : libpython2.7-minimal_2.7.9-2+deb8u3
Remote package installed : libpython2.7-stdlib_2.7.9-2+deb8u2
Should be : libpython2.7-stdlib_2.7.9-2+deb8u3
Remote package installed : python2.7_2.7.9-2+deb8u2
Should be : python2.7_2.7.9-2+deb8u3
Remote package installed : python2.7-minimal_2.7.9-2+deb8u2
Should be : python2.7-minimal_2.7.9-2+deb8u3
```

126833 - Debian DLA-1856-1 : patch security update

Synopsis

The remote Debian host is missing a security update.

Description

Handling of symlinks in patch, a tool to apply a diff file to an original, was wrong in certain cases.

For Debian 8 'Jessie', this problem has been fixed in version 2.7.5-1+deb8u2.

We recommend that you upgrade your patch 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/2019/07/msg00016.html
https://packages.debian.org/source/jessie/patch

Solution

Upgrade the affected patch package.

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

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-13636

Plugin Information

Published: 2019/07/22, Modified: 2025/02/25

Plugin Output

tcp/0

```
Remote package installed : patch_2.7.5-1
Should be : patch_2.7.5-1+deb8u2
```

126836 - Debian DLA-1859-1 : bind9 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was found in the Bind DNS Server. Limits on simultaneous tcp connections have not been enforced correctly and could lead to exhaustion of file descriptors. In the worst case this could affect the file descriptors of the whole system.

For Debian 8 'Jessie', this problem has been fixed in version 1:9.9.5.dfsg-9+deb8u18.

We recommend that you upgrade your bind9 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/2019/07/msg00019.html
https://packages.debian.org/source/jessie/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)

References

CVE CVE-2018-5743

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.9.5.dfsg-9+deb8u17
Should be : bind9-host_1:9.9.5.dfsg-9+deb8u18
Remote package installed : dnsutils_1:9.9.5.dfsg-9+deb8u17
Should be : dnsutils_1:9.9.5.dfsg-9+deb8u18
Remote package installed : host_1:9.9.5.dfsg-9+deb8u17
Should be : host_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libbind9-90_1:9.9.5.dfsg-9+deb8u17
Should be : libbind9-90_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libdns-export100_1:9.9.5.dfsg-9+deb8u17
Should be : libdns-export100_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libdns100_1:9.9.5.dfsg-9+deb8u17
Should be : libdns100_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libirs-export91_1:9.9.5.dfsg-9+deb8u17
Should be : libirs-export91_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libisc-export95_1:9.9.5.dfsg-9+deb8u17
Should be : libisc-export95_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libisc95_1:9.9.5.dfsg-9+deb8u17
Should be : libisc95_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libisccc90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccc90_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libisccfg-export90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccfg-export90_1:9.9.5.dfsg-9+deb8u18
Remote package installed : libisccfg90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccfg90_1:9.9.5.dfsg-9+deb8u18
Remote package installed : liblwres90_1:9.9.5.dfsg-9+deb8u17
Should be : liblwres90_1:9.9.5.dfsg-9+deb8u18
```

127475 - Debian DLA-1866-2 : glib2.0 regression update -

Synopsis

The remote Debian host is missing a security update.

Description

Simon McVittie spotted a memory leak regression in the way CVE-2019-13012 had been resolved for glib2.0 in Debian jessie.

For Debian 8 'Jessie', this problem has been fixed in version 2.42.1-1+deb8u3.

We recommend that you upgrade your glib2.0 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/2019/08/msg00004.html
https://packages.debian.org/source/jessie/glib2.0

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

6.5 (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-2019-13012

Plugin Information

Published: 2019/08/12, Modified: 2024/05/07

Plugin Output

tcp/0

```
Remote package installed : libglib2.0-0_2.42.1-1+b1
Should be : libglib2.0-0_2.42.1-1+deb8u3
Remote package installed : libglib2.0-data_2.42.1-1
Should be : libglib2.0-data_2.42.1-1+deb8u3
```

127820 - Debian DLA-1878-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two heap buffer overflows were found in the EXIF parsing code of PHP, a widely-used open source general purpose scripting language.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u5.

We recommend that you upgrade your php5 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/2019/08/msg00010.html
https://packages.debian.org/source/jessie/php5

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.4 (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-2019-11041
CVE	CVE-2019-11042

Plugin Information

Published: 2019/08/13, Modified: 2024/05/06

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u5
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u5
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u5
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u5
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u5
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u5
```

127927 - Debian DLA-1891-1 : openldap security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several security vulnerabilities were discovered in openldap, a server and tools to provide a standalone directory service.

CVE-2019-13057

When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control.
(It is not a common configuration to deploy a system where the server administrator and a DB administrator enjoy different levels of trust.)

CVE-2019-13565

When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user affects the authorization requirement for a different user.

For Debian 8 'Jessie', these problems have been fixed in version 2.4.40+dfsg-1+deb8u5.

We recommend that you upgrade your openldap 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/2019/08/msg00024.html
https://packages.debian.org/source/jessie/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:H/I:N/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:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-13057
CVE	CVE-2019-13565

Plugin Information

Published: 2019/08/20, Modified: 2024/05/02

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.40+dfsg-1+deb8u3
Should be : libldap-2.4-2_2.4.40+dfsg-1+deb8u5
```

128082 - Debian DLA-1893-1 : cups security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two issues have been found in cups, the Common UNIX Printing System(tm).

Basically both CVEs (CVE-2019-8675 and CVE-2019-8696) are about stack-buffer-overflow in two functions of libcup. One happens in asn1_get_type() the other one in asn1_get_packed().

For Debian 8 'Jessie', these problems have been fixed in version 1.7.5-11+deb8u5.

We recommend that you upgrade your cups 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/2019/08/msg00026.html
https://packages.debian.org/source/jessie/cups

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-8675
CVE	CVE-2019-8696

Plugin Information

Published: 2019/08/23, Modified: 2024/05/02

Plugin Output

tcp/0

```
Remote package installed : libcups2_1.7.5-11+deb8u4
Should be : libcups2_1.7.5-11+deb8u5
```

128124 - Debian DLA-1897-1 : tiff security update -

Synopsis

The remote Debian host is missing a security update.

Description

Even Rouault found an issue in tiff, a library providing support for the Tag Image File Format. Wrong handling off integer overflow checks, that are based on undefined compiler behavior, might result in an application crash.

For Debian 8 'Jessie', this problem has been fixed in version 4.0.3-12.3+deb8u9.

We recommend that you upgrade your tiff 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/2019/08/msg00031.html
https://packages.debian.org/source/jessie/tiff

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-14973

Plugin Information

Published: 2019/08/26, Modified: 2024/05/02

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.3-12.3+deb8u8
Should be : libtiff5_4.0.3-12.3+deb8u9
```

128426 - Debian DLA-1906-1 : python2.7 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability has been discovered in Python, an interactive high-level object-oriented language, that is relevant for cookie handling. By using a malicious server an attacker might steal cookies that are meant for other domains

For Debian 8 'Jessie', this problem has been fixed in version 2.7.9-2+deb8u4.

We recommend that you upgrade your python2.7 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/2019/08/msg00040.html
https://packages.debian.org/source/jessie/python2.7

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-2018-20852

Plugin Information

Published: 2019/09/03, Modified: 2024/04/30

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.9-2+deb8u2
Should be : libpython2.7-minimal_2.7.9-2+deb8u4
Remote package installed : libpython2.7-stdlib_2.7.9-2+deb8u2
Should be : libpython2.7-stdlib_2.7.9-2+deb8u4
Remote package installed : python2.7_2.7.9-2+deb8u2
Should be : python2.7_2.7.9-2+deb8u4
Remote package installed : python2.7-minimal_2.7.9-2+deb8u2
Should be : python2.7-minimal_2.7.9-2+deb8u4
```

128509 - Debian DLA-1909-1 : freetype security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several newly-referenced issues have been fixed in the FreeType 2 font engine.

CVE-2015-9381

heap-based buffer over-read in T1_Get_Private_Dict in type1/t1parse.c

CVE-2015-9382

buffer over-read in skip_comment in psaux/psobjs.c because ps_parser_skip_PS_token is mishandled in an FT_New_Memory_Face operation

CVE-2015-9383

a heap-based buffer over-read in tt_cmap14_validate in sfnt/ttcmap.c

For Debian 8 'Jessie', these problems have been fixed in version 2.5.2-3+deb8u4.

We recommend that you upgrade your freetype 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/2019/09/msg00002.html
https://packages.debian.org/source/jessie/freetype

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-2015-9381
CVE	CVE-2015-9382
CVE	CVE-2015-9383

Plugin Information

Published: 2019/09/05, Modified: 2024/04/29

Plugin Output

tcp/0

```
Remote package installed : libfreetype6_2.5.2-3+deb8u2
Should be : libfreetype6_2.5.2-3+deb8u4
```

128778 - Debian DLA-1918-1 : libonig security update -

Synopsis

The remote Debian host is missing a security update.

Description

The Oniguruma regular expressions library, notably used in PHP mbstring, is vulnerable to stack exhaustion. A crafted regular expression can crash the process.

For Debian 8 'Jessie', this problem has been fixed in version 5.9.5-3.2+deb8u3.

We recommend that you upgrade your libonig 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/2019/09/msg00010.html
https://packages.debian.org/source/jessie/libonig

Solution

Upgrade the affected libonig-dev, libonig2, and libonig2-dbg 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-2019-16163

Plugin Information

Published: 2019/09/16, Modified: 2024/04/26

Plugin Output

tcp/0

```
Remote package installed : libonig2_5.9.5-3.2+deb8u1
Should be : libonig2_5.9.5-3.2+deb8u3
```

128883 - Debian DLA-1925-1 : python2.7 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in Python, an interactive high-level object-oriented language.

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.

For Debian 8 'Jessie', this problem has been fixed in version 2.7.9-2+deb8u5.

We recommend that you upgrade your python2.7 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/2019/09/msg00019.html
https://packages.debian.org/source/jessie/python2.7

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-16056

Plugin Information

Published: 2019/09/17, Modified: 2024/04/25

Plugin Output

tcp/0

```
Remote package installed : libpython2.7-minimal_2.7.9-2+deb8u2
Should be : libpython2.7-minimal_2.7.9-2+deb8u5
Remote package installed : libpython2.7-stdlib_2.7.9-2+deb8u2
Should be : libpython2.7-stdlib_2.7.9-2+deb8u5
Remote package installed : python2.7_2.7.9-2+deb8u2
Should be : python2.7_2.7.9-2+deb8u5
Remote package installed : python2.7-minimal_2.7.9-2+deb8u2
Should be : python2.7-minimal_2.7.9-2+deb8u5
```

129362 - Debian DLA-1932-1 : openssl security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two security vulnerabilities were found in OpenSSL, the Secure Sockets Layer toolkit.

CVE-2019-1547

Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation.
In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used.

CVE-2019-1563

In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt.

For Debian 8 'Jessie', these problems have been fixed in version 1.0.1t-1+deb8u12.

We recommend that you upgrade your openssl 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/2019/09/msg00026.html
https://packages.debian.org/source/jessie/openssl

Solution

Upgrade the affected packages.

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

Plugin Information

Published: 2019/09/26, Modified: 2024/04/23

Plugin Output

tcp/0

```
Remote package installed : libssl1.0.0_1.0.1t-1+deb8u11
Should be : libssl1.0.0_1.0.1t-1+deb8u12
Remote package installed : openssl_1.0.1t-1+deb8u11
Should be : openssl_1.0.1t-1+deb8u12
```

129409 - Debian DLA-1935-1 : e2fsprogs security update -

Synopsis

The remote Debian host is missing a security 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.

For Debian 8 'Jessie', this problem has been fixed in version 1.42.12-2+deb8u1.

We recommend that you upgrade your e2fsprogs 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/2019/09/msg00029.html
https://packages.debian.org/source/jessie/e2fsprogs

Solution

Upgrade the affected packages.

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

Plugin Information

Published: 2019/09/30, Modified: 2025/06/02

Plugin Output

tcp/0

```
Remote package installed : e2fslibs_1.42.12-2+b1
Should be : e2fslibs_1.42.12-2+deb8u1
Remote package installed : e2fsprogs_1.42.12-2+b1
Should be : e2fsprogs_1.42.12-2+deb8u1
Remote package installed : libcomerr2_1.42.12-2+b1
Should be : libcomerr2_1.42.12-2+deb8u1
Remote package installed : libss2_1.42.12-2+b1
Should be : libss2_1.42.12-2+deb8u1
```

129410 - Debian DLA-1936-1 : cups security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in cups, the Common UNIX Printing System(tm).

While generating a session cookie for the CUPS web interface, a predictable random number seed was used. This could lead to unauthorized scripted access to the enabled web interface.

For Debian 8 'Jessie', this problem has been fixed in version 1.7.5-11+deb8u6.

We recommend that you upgrade your cups 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/2019/09/msg00028.html
https://packages.debian.org/source/jessie/cups

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:H/I:N/A:N)

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:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2018-4300

Plugin Information

Published: 2019/09/30, Modified: 2025/02/24

Plugin Output

tcp/0

```
Remote package installed : libcups2_1.7.5-11+deb8u4
Should be : libcups2_1.7.5-11+deb8u6
```

130182 - Debian DLA-1969-1 : file security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in file, a tool to determine file types by using magic numbers.

The number of CDF_VECTOR elements had to be restricted in order to prevent a heap-based buffer overflow (4-byte out-of-bounds write).

For Debian 8 'Jessie', this problem has been fixed in version 1:5.22+15-2+deb8u6.

We recommend that you upgrade your file 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/2019/10/msg00032.html
https://packages.debian.org/source/jessie/file

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-2019-18218

Plugin Information

Published: 2019/10/24, Modified: 2024/04/17

Plugin Output

tcp/0

```
Remote package installed : file_1:5.22+15-2+deb8u5
Should be : file_1:5.22+15-2+deb8u6
Remote package installed : libmagic1_1:5.22+15-2+deb8u5
Should be : libmagic1_1:5.22+15-2+deb8u6
```

130286 - Debian DLA-1973-1 : libxslt security update -

Synopsis

The remote Debian host is missing a security update.

Description

A security vulnerability was discovered in libxslt, a XSLT 1.0 processing library written in C.

In xsltCopyText in transform.c, a pointer variable is not reset under certain circumstances. If the relevant memory area happened to be freed and reused in a certain way, a bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed.

For Debian 8 'Jessie', this problem has been fixed in version 1.1.28-2+deb8u6.

We recommend that you upgrade your libxslt 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/2019/10/msg00037.html
https://packages.debian.org/source/jessie/libxslt

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-18197

Plugin Information

Published: 2019/10/28, Modified: 2024/04/16

Plugin Output

tcp/0

```
Remote package installed : libxslt1.1_1.1.28-2+deb8u4
Should be : libxslt1.1_1.1.28-2+deb8u6
```

130522 - Debian DLA-1981-1 : cpio security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in the cpio package.

CVE-2019-14866

It is possible for an attacker to create a file so when backed up with cpio can generate arbitrary files in the resulting tar archive. When the backup is restored the file is then created with arbitrary permissions.

For Debian 8 'Jessie', this problem has been fixed in version 2.11+dfsg-4.1+deb8u2.

We recommend that you upgrade your cpio 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/2019/11/msg00001.html
https://packages.debian.org/source/jessie/cpio

Solution

Upgrade the affected cpio, and cpio-win32 packages.

Risk Factor

Medium

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

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-2019-14866

Plugin Information

Published: 2019/11/06, Modified: 2024/04/16

Plugin Output

tcp/0

```
Remote package installed : cpio_2.11+dfsg-4.1+deb8u1
Should be : cpio_2.11+dfsg-4.1+deb8u2
```

130980 - Debian DLA-1991-1 : libssh2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

In libssh2, 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 8 'Jessie', this problem has been fixed in version 1.4.3-4.1+deb8u6.

We recommend that you upgrade your libssh2 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/2019/11/msg00010.html
https://packages.debian.org/source/jessie/libssh2

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-2019-17498

Plugin Information

Published: 2019/11/14, Modified: 2024/04/11

Plugin Output

tcp/0

```
Remote package installed : libssh2-1_1.4.3-4.1+deb8u3
Should be : libssh2-1_1.4.3-4.1+deb8u6
```

131328 - Debian DLA-2009-1 : tiff security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several issues have been found in tiff, a Tag Image File Format library.

CVE-2019-17546

The RGBA interface contains an integer overflow that might lead to heap buffer overflow write.

CVE-2019-6128

A memory leak exists due to missing cleanup code.

CVE-2018-18661

In case of exhausted memory there is a NULL pointer dereference in tiff2bw.

CVE-2018-12900

Fix for heap-based buffer overflow, that could be used to crash an application or even to execute arbitrary code (with the permission of the user running this application).

CVE-2017-17095

A crafted tiff file could lead to a heap buffer overflow in pal2rgb.

For Debian 8 'Jessie', these problems have been fixed in version 4.0.3-12.3+deb8u10.

We recommend that you upgrade your tiff 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/2019/11/msg00027.html
https://packages.debian.org/source/jessie/tiff

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-2017-17095
CVE	CVE-2018-12900
CVE	CVE-2018-18661
CVE	CVE-2019-17546
CVE	CVE-2019-6128

Plugin Information

Published: 2019/11/27, Modified: 2024/04/09

Plugin Output

tcp/0

```
Remote package installed : libtiff5_4.0.3-12.3+deb8u8
Should be : libtiff5_4.0.3-12.3+deb8u10
```

131331 - Debian DLA-2012-1 : libvpx security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several issues have been found in libvpx, a VP8 and VP9 video codec.

CVE-2019-9232

There is a possible out of bounds read due to a missing bounds check.
This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE-2019-9433

There is a possible information disclosure due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.

For Debian 8 'Jessie', these problems have been fixed in version 1.3.0-3+deb8u2.

We recommend that you upgrade your libvpx 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/2019/11/msg00030.html
https://packages.debian.org/source/jessie/libvpx

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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-9232
CVE	CVE-2019-9433

Plugin Information

Published: 2019/11/27, Modified: 2024/04/09

Plugin Output

tcp/0

```
Remote package installed : libvpx1_1.3.0-3+deb8u1
Should be : libvpx1_1.3.0-3+deb8u2
```

132325 - Debian DLA-2043-2 : gdk-pixbuf regression update -

Synopsis

The remote Debian host is missing a security update.

Description

While preparing a fix for CVE-2017-6314 an unknown symbol g_uint_checked_mul() was introduced.

For Debian 8 'Jessie', this problem has been fixed in version 2.31.1-2+deb8u9.

We recommend that you upgrade your gdk-pixbuf 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/2019/12/msg00026.html
https://packages.debian.org/source/jessie/gdk-pixbuf

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)

Plugin Information

Published: 2019/12/20, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : libgdk-pixbuf2.0-0_2.31.1-2+deb8u7
Should be : libgdk-pixbuf2.0-0_2.31.1-2+deb8u9
Remote package installed : libgdk-pixbuf2.0-common_2.31.1-2+deb8u7
Should be : libgdk-pixbuf2.0-common_2.31.1-2+deb8u9
```

132344 - Debian DLA-2044-1 : cyrus-sasl2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

There has been an out-of-bounds write in Cyrus SASL leading to unauthenticated remote denial of service in OpenLDAP via a malformed LDAP packet. The OpenLDAP crash was ultimately caused by an off-by-one error in _sasl_add_string in common.c in cyrus-sasl.

For Debian 8 'Jessie', this problem has been fixed in version 2.1.26.dfsg1-13+deb8u2.

We recommend that you upgrade your cyrus-sasl2 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/2019/12/msg00027.html
https://packages.debian.org/source/jessie/cyrus-sasl2

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-2019-19906

Plugin Information

Published: 2019/12/23, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : libsasl2-2_2.1.26.dfsg1-13+deb8u1
Should be : libsasl2-2_2.1.26.dfsg1-13+deb8u2
Remote package installed : libsasl2-modules_2.1.26.dfsg1-13+deb8u1
Should be : libsasl2-modules_2.1.26.dfsg1-13+deb8u2
Remote package installed : libsasl2-modules-db_2.1.26.dfsg1-13+deb8u1
Should be : libsasl2-modules-db_2.1.26.dfsg1-13+deb8u2
```

132346 - Debian DLA-2047-1 : cups security update -

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in cups, the Common UNIX Printing System(tm).

An incorrect bounds check could lead to a possible out-of-bounds read and local information disclosure in the printer spooler.

For Debian 8 'Jessie', this problem has been fixed in version 1.7.5-11+deb8u7.

We recommend that you upgrade your cups 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/2019/12/msg00030.html
https://packages.debian.org/source/jessie/cups

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-2228

Plugin Information

Published: 2019/12/23, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : libcups2_1.7.5-11+deb8u4
Should be : libcups2_1.7.5-11+deb8u7
```

132420 - Debian DLA-2048-1 : libxml2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a potential denial of service vulnerability in libxml2, the GNOME XML parsing library.

For Debian 8 'Jessie', this issue has been fixed in libxml2 version 2.9.1+dfsg1-5+deb8u8.

We recommend that you upgrade your libxml2 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/2019/12/msg00032.html
https://packages.debian.org/source/jessie/libxml2

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-2019-19956

Plugin Information

Published: 2019/12/30, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : libxml2_2.9.1+dfsg1-5+deb8u7
Should be : libxml2_2.9.1+dfsg1-5+deb8u8
```

132422 - Debian DLA-2050-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several security bugs have been identified and fixed in php5, a server-side, HTML-embedded scripting language. The affected components include the exif module and handling of filenames with \0 embedded.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u8.

We recommend that you upgrade your php5 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/2019/12/msg00034.html
https://packages.debian.org/source/jessie/php5

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (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

Plugin Information

Published: 2019/12/30, Modified: 2024/04/02

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u8
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u8
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u8
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u8
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u8
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u8
```

133324 - Debian DLA-2086-1 : wget security update

Synopsis

The remote Debian host is missing a security update.

Description

An issue has been found in wget, a tool to retrieve files from the web. A race condition might occur as files rejected by an access list are kept on the disk for the duration of a HTTP connection.

For Debian 8 'Jessie', this problem has been fixed in version 1.16-1+deb8u7.

We recommend that you upgrade your wget 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/2020/01/msg00031.html
https://packages.debian.org/source/jessie/wget

Solution

Upgrade the affected wget package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2016-7098

Plugin Information

Published: 2020/01/30, Modified: 2025/02/21

Plugin Output

tcp/0

```
Remote package installed : wget_1.16-1+deb8u5
Should be : wget_1.16-1+deb8u7
```

133730 - Debian DLA-2106-1 : libgd2 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability was discovered in libgd2, the GD graphics library, whereby an attacker can employ a specific function call sequence to trigger a NULL pointer dereference, subsequently crash the application using libgd2, and create a denial of service.

For Debian 8 'Jessie', this problem has been fixed in version 2.1.0-5+deb8u14.

We recommend that you upgrade your libgd2 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/2020/02/msg00014.html
https://packages.debian.org/source/jessie/libgd2

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)

References

CVE CVE-2018-14553

Plugin Information

Published: 2020/02/18, Modified: 2024/03/27

Plugin Output

tcp/0

```
Remote package installed : libgd3_2.1.0-5+deb8u12
Should be : libgd3_2.1.0-5+deb8u14
```

134175 - Debian DLA-2124-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two issues have been found in php5, a server-side, HTML-embedded scripting language. Both issues are related to crafted data that could lead to reading after an allocated buffer and result in information disclosure or crash.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u9.

We recommend that you upgrade your php5 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/2020/02/msg00030.html
https://packages.debian.org/source/jessie/php5

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-2020-7059
CVE	CVE-2020-7060

Plugin Information

Published: 2020/03/02, Modified: 2024/03/25

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u9
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u9
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u9
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u9
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u9
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u9
```

134768 - Debian DLA-2151-1 : icu security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that an integer overflow in the International Components for Unicode (ICU) library could result in denial of service and potentially the execution of arbitrary code.

For Debian 8 'Jessie', this problem has been fixed in version 52.1-8+deb8u8.

We recommend that you upgrade your icu 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/2020/03/msg00024.html
https://packages.debian.org/source/jessie/icu

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

7.7 (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

Plugin Information

Published: 2020/03/23, Modified: 2024/03/21

Plugin Output

tcp/0

```
Remote package installed : libicu52_52.1-8+deb8u7
Should be : libicu52_52.1-8+deb8u8
```

134880 - Debian DLA-2156-1 : 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 8 'Jessie', this problem has been fixed in version 1.42.12-2+deb8u2.

We recommend that you upgrade your e2fsprogs 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/2020/03/msg00030.html
https://packages.debian.org/source/jessie/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: 2020/03/25, Modified: 2024/03/21

Plugin Output

tcp/0

```
Remote package installed : e2fslibs_1.42.12-2+b1
Should be : e2fslibs_1.42.12-2+deb8u2
Remote package installed : e2fsprogs_1.42.12-2+b1
Should be : e2fsprogs_1.42.12-2+deb8u2
Remote package installed : libcomerr2_1.42.12-2+b1
Should be : libcomerr2_1.42.12-2+deb8u2
Remote package installed : libss2_1.42.12-2+b1
Should be : libss2_1.42.12-2+deb8u2
```

134955 - Debian DLA-2160-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two security issues have been identified and fixed in php5, a server-side, HTML-embedded scripting language.

CVE-2020-7062 is about a possible NULL pointer derefernce, which would likely lead to a crash, during a failed upload with progress tracking.
CVE-2020-7063 is about wrong file permissions of files added to tar with Phar::buildFromIterator when extracting them again.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u10.

We recommend that you upgrade your php5 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/2020/03/msg00034.html
https://packages.debian.org/source/jessie/php5

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)

References

CVE	CVE-2020-7062
CVE	CVE-2020-7063

Plugin Information

Published: 2020/03/27, Modified: 2024/03/20

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u10
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u10
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u10
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
```

```
Should be : php5-common_5.6.40+dfsg-0+deb8u10
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u10
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u10
```

135980 - Debian DLA-2188-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

Three issues have been found in php5, a server-side, HTML-embedded scripting language.

CVE-2020-7064 A one byte out-of-bounds read, which could potentially lead to information disclosure or crash.

CVE-2020-7066 An URL containing zero (\0) character will be truncated at it, which may cause some software to make incorrect assumptions and possibly send some information to a wrong server.

CVE-2020-7067 Using a malformed url-encoded string an Out-of-Bounds read can occur.

For Debian 8 'Jessie', these problems have been fixed in version 5.6.40+dfsg-0+deb8u11.

We recommend that you upgrade your php5 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/2020/04/msg00021.html
https://packages.debian.org/source/jessie/php5

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

5.8 (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)

STIG Severity

I

References

CVE	CVE-2020-7064
CVE	CVE-2020-7066
CVE	CVE-2020-7067
XREF	IAVA:2020-A-0169-S
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/04/27, Modified: 2024/03/14

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u11
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u11
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u11
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u11
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u11
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u11
```

136204 - Debian DLA-2195-1 : w3m security update -

Synopsis

The remote Debian host is missing a security update.

Description

Two issues have been found in w3m, WWW browsable pager with excellent tables/frames support.

One issue is related to a stack overflow, the other one is a fix for a NULL pointer dereference.

Brief introduction

CVE-2018-6196

Description

CVE-2018-6197

Description

For Debian 8 'Jessie', these problems have been fixed in version 0.5.3-19+deb8u3.

We recommend that you upgrade your w3m 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/2020/04/msg00025.html
https://packages.debian.org/source/jessie/w3m

Solution

Upgrade the affected w3m, and w3m-img 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-2018-6196
CVE	CVE-2018-6197

Plugin Information

Published: 2020/05/01, Modified: 2024/03/14

Plugin Output

tcp/0

```
Remote package installed : w3m_0.5.3-19+deb8u2
Should be : w3m_0.5.3-19+deb8u3
```

136289 - Debian DLA-2199-1 : openldap security update -

Synopsis

The remote Debian host is missing a security 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).

For Debian 8 'Jessie', this problem has been fixed in version 2.4.40+dfsg-1+deb8u6.

We recommend that you upgrade your openldap 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/2020/05/msg00001.html
https://packages.debian.org/source/jessie/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)

STIG Severity

I

References

CVE	CVE-2020-12243
XREF	IAVB:2020-B-0028-S

Plugin Information

Published: 2020/05/04, Modified: 2024/03/13

Plugin Output

tcp/0

```
Remote package installed : libldap-2.4-2_2.4.40+dfsg-1+deb8u3
Should be : libldap-2.4-2_2.4.40+dfsg-1+deb8u6
```

136368 - Debian DLA-2203-1 : sqlite3 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a denial of service attack in the SQLite database, often embedded into other programs and servers.

In the event of a semantic error in an aggregate query, SQLite did not return early from the 'resetAccumulator()' function which would lead to a crash via a segmentation fault.

For Debian 8 'Jessie', this issue has been fixed in sqlite3 version 3.8.7.1-1+deb8u5.

We recommend that you upgrade your sqlite3 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/2020/05/msg00006.html
https://packages.debian.org/source/jessie/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

6.7 (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-2020-11655

Plugin Information

Published: 2020/05/07, Modified: 2024/03/13

Plugin Output

tcp/0

```
Remote package installed : libsqlite3-0_3.8.7.1-1+deb8u4
Should be : libsqlite3-0_3.8.7.1-1+deb8u5
```

136631 - Debian DLA-2210-1 : apt security update -

Synopsis

The remote Debian host is missing a security update.

Description

When normalizing ar member names by removing trailing whitespace and slashes, an out-out-bound read can be caused if the ar member name consists only of such characters, because the code did not stop at 0, but would wrap around and continue reading from the stack, without any limit.

For Debian 8 'Jessie', this problem has been fixed in version 1.0.9.8.6.

We recommend that you upgrade your apt 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/2020/05/msg00013.html
https://packages.debian.org/source/jessie/apt

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-2020-3810

Plugin Information

Published: 2020/05/15, Modified: 2024/03/12

Plugin Output

tcp/0

```
Remote package installed : apt_1.0.9.8.5
Should be : apt_1.0.9.8.6
Remote package installed : apt-utils_1.0.9.8.5
Should be : apt-utils_1.0.9.8.6
Remote package installed : libapt-inst1.5_1.0.9.8.5
Should be : libapt-inst1.5_1.0.9.8.6
Remote package installed : libapt-pkg4.12_1.0.9.8.5
Should be : libapt-pkg4.12_1.0.9.8.6
```

136702 - Debian DLA-2213-1 : exim4 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that exim4, a mail transport agent, suffers from a authentication bypass vulnerability in the spa authentication driver.
The spa authentication driver is not enabled by default.

For Debian 8 'Jessie', this problem has been fixed in version 4.84.2-2+deb8u7.

We recommend that you upgrade your exim4 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/2020/05/msg00017.html
https://packages.debian.org/source/jessie/exim4

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)

References

CVE CVE-2020-12783

Plugin Information

Published: 2020/05/19, Modified: 2024/03/12

Plugin Output

tcp/0

```
Remote package installed : exim4_4.84.2-2+deb8u5
Should be : exim4_4.84.2-2+deb8u7
Remote package installed : exim4-base_4.84.2-2+deb8u5
Should be : exim4-base_4.84.2-2+deb8u7
Remote package installed : exim4-config_4.84.2-2+deb8u5
Should be : exim4-config_4.84.2-2+deb8u7
Remote package installed : exim4-daemon-light_4.84.2-2+deb8u5
Should be : exim4-daemon-light_4.84.2-2+deb8u7
```

136983 - Debian DLA-2227-1 : 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-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.

For Debian 8 'Jessie', these problems have been fixed in version 1:9.9.5.dfsg-9+deb8u19.

We recommend that you upgrade your bind9 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/2020/05/msg00031.html
https://packages.debian.org/source/jessie/bind9

Solution

Upgrade the affected packages.

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)

References

CVE	CVE-2020-8616
CVE	CVE-2020-8617

Plugin Information

Published: 2020/06/01, Modified: 2024/03/08

Plugin Output

tcp/0

```
Remote package installed : bind9-host_1:9.9.5.dfsg-9+deb8u17
Should be : bind9-host_1:9.9.5.dfsg-9+deb8u19
Remote package installed : dnsutils_1:9.9.5.dfsg-9+deb8u17
Should be : dnsutils_1:9.9.5.dfsg-9+deb8u19
Remote package installed : host_1:9.9.5.dfsg-9+deb8u17
Should be : host_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libbind9-90_1:9.9.5.dfsg-9+deb8u17
Should be : libbind9-90_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libdns-export100_1:9.9.5.dfsg-9+deb8u17
Should be : libdns-export100_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libdns100_1:9.9.5.dfsg-9+deb8u17
Should be : libdns100_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libirs-export91_1:9.9.5.dfsg-9+deb8u17
Should be : libirs-export91_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libisc-export95_1:9.9.5.dfsg-9+deb8u17
Should be : libisc-export95_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libisc95_1:9.9.5.dfsg-9+deb8u17
Should be : libisc95_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libisccc90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccc90_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libisccfg-export90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccfg-export90_1:9.9.5.dfsg-9+deb8u19
Remote package installed : libisccfg90_1:9.9.5.dfsg-9+deb8u17
Should be : libisccfg90_1:9.9.5.dfsg-9+deb8u19
Remote package installed : liblwres90_1:9.9.5.dfsg-9+deb8u17
Should be : liblwres90_1:9.9.5.dfsg-9+deb8u19
```

136984 - Debian DLA-2228-2 : json-c regression update -

Synopsis

The remote Debian host is missing a security update.

Description

The json-c shared library had an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.

This follow-up version now uses an upstream sanctioned patch that was specifically published for json-c 0.11, rather than a self-backported patch.

For Debian 8 'Jessie', this problem has been fixed in version 0.11-4+deb8u2.

We recommend that you upgrade your json-c 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/2020/05/msg00034.html
https://packages.debian.org/source/jessie/json-c

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-2020-12762

Plugin Information

Published: 2020/06/01, Modified: 2024/03/08

Plugin Output

tcp/0

```
Remote package installed : libjson-c2_0.11-4
Should be : libjson-c2_0.11-4+deb8u2
```

137205 - Debian DLA-2235-1 : dbus security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that there was a file descriptor leak in the D-Bus message bus.

An unprivileged local attacker could use this to attack the system DBus daemon, leading to denial of service for all users of the machine.

For Debian 8 'Jessie', this issue has been fixed in dbus version 1.8.22-0+deb8u3.

We recommend that you upgrade your dbus 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/2020/06/msg00003.html
https://packages.debian.org/source/jessie/dbus

Solution

Upgrade the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-12049

Plugin Information

Published: 2020/06/08, Modified: 2024/03/07

Plugin Output

tcp/0

```
Remote package installed : dbus_1.8.22-0+deb8u1
Should be : dbus_1.8.22-0+deb8u3
Remote package installed : libdbus-1-3_1.8.22-0+deb8u1
Should be : libdbus-1-3_1.8.22-0+deb8u3
```

137207 - Debian DLA-2237-1 : cups security update -

Synopsis

The remote Debian host is missing a security update.

Description

The following CVE(s) were reported against src:cups.

CVE-2019-8842

The `ippReadIO` function may under-read an extension field.

CVE-2020-3898

There was a heap based buffer overflow in libcups's ppdFindOption() in ppd-mark.c. The `ppdOpen` function did not handle invalid UI constraint. `ppdcSource::get_resolution` function did not handle invalid resolution strings.

For Debian 8 'Jessie', these problems have been fixed in version 1.7.5-11+deb8u8.

We recommend that you upgrade your cups 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/2020/06/msg00005.html
https://packages.debian.org/source/jessie/cups

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

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-2019-8842
CVE	CVE-2020-3898

Plugin Information

Published: 2020/06/08, Modified: 2024/03/07

Plugin Output

tcp/0

```
Remote package installed : libcups2_1.7.5-11+deb8u4
Should be : libcups2_1.7.5-11+deb8u8
```

137858 - Debian DLA-2255-1 : libtasn1-6 security update -

Synopsis

The remote Debian host is missing a security update.

Description

A vulnerability has been discovered in Libtasn1, a library to manage ASN.1 structures, allowing a remote attacker to cause a denial of service against an application using the Libtasn1 library.

For Debian 8 'Jessie', this problem has been fixed in version 4.2-3+deb8u4.

We recommend that you upgrade your libtasn1-6 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/2020/06/msg00026.html
https://packages.debian.org/source/jessie/libtasn1-6

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-2017-10790

Plugin Information

Published: 2020/06/29, Modified: 2024/03/05

Plugin Output

tcp/0

```
Remote package installed : libtasn1-6_4.2-3+deb8u3
Should be : libtasn1-6_4.2-3+deb8u4
```

137859 - Debian DLA-2256-1 : libtirpc security update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that libtiprc, a transport-independent RPC library, could be used for a denial of service or possibly unspecified other impact by a stack-based buffer overflow due to a flood of crafted ICMP and UDP packets.

For Debian 8 'Jessie', this problem has been fixed in version 0.2.5-1+deb8u3.

We recommend that you upgrade your libtirpc 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/2020/06/msg00027.html
https://packages.debian.org/source/jessie/libtirpc

Solution

Upgrade the affected libtirpc-dev, and libtirpc1 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)

References

CVE CVE-2016-4429

Plugin Information

Published: 2020/06/29, Modified: 2024/03/05

Plugin Output

tcp/0

```
Remote package installed : libtirpc1_0.2.5-1+deb8u2
Should be : libtirpc1_0.2.5-1+deb8u3
```

137886 - Debian DLA-2261-1 : php5 security update -

Synopsis

The remote Debian host is missing a security update.

Description

It has been discovered, that a vulnerability in php5, a server-side, HTML-embedded scripting language, could lead to exhausted disk space on the server. When using overly long filenames or field names, a memory limit could be hit which results in stopping the upload but not cleaning up behind.

Further the embedded version of 'file' is vulnerable to CVE-2019-18218. As it can not be exploited the same in php5 as in file, this issue is not handled as an own CVE but just as a bug, that has been fixed here (restrict the number of CDF_VECTOR elements to prevent a heap-based buffer overflow (4-byte out-of-bounds write)).

For Debian 8 'Jessie', this problem has been fixed in version 5.6.40+dfsg-0+deb8u12.

We recommend that you upgrade your php5 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/2020/06/msg00033.html
https://packages.debian.org/source/jessie/php5

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-2019-11048

Plugin Information

Published: 2020/06/30, Modified: 2024/03/05

Plugin Output

tcp/0

```
Remote package installed : php5_5.6.40+dfsg-0+deb8u2
Should be : php5_5.6.40+dfsg-0+deb8u12
Remote package installed : php5-cgi_5.6.40+dfsg-0+deb8u2
Should be : php5-cgi_5.6.40+dfsg-0+deb8u12
Remote package installed : php5-cli_5.6.40+dfsg-0+deb8u2
Should be : php5-cli_5.6.40+dfsg-0+deb8u12
Remote package installed : php5-common_5.6.40+dfsg-0+deb8u2
Should be : php5-common_5.6.40+dfsg-0+deb8u12
Remote package installed : php5-fpm_5.6.40+dfsg-0+deb8u2
Should be : php5-fpm_5.6.40+dfsg-0+deb8u12
Remote package installed : php5-readline_5.6.40+dfsg-0+deb8u2
Should be : php5-readline_5.6.40+dfsg-0+deb8u12
```

137911 - Debian DLA-2268-2 : mutt regression update -

Synopsis

The remote Debian host is missing a security update.

Description

Two vulnerabilities have been discovered in mutt, a console email client.

CVE-2020-14093

Mutt allowed an IMAP fcc/postpone man-in-the-middle attack via a PREAUTH response.

CVE-2020-14954

Mutt had a STARTTLS buffering issue that affected IMAP, SMTP, and POP3. When a server had sent a 'begin TLS' response, the client read additional data (e.g., from a man-in-the-middle attacker) and evaluated it in a TLS context, aka 'response injection.'

In Debian jessie, the mutt source package builds two variants of mutt:
mutt and mutt-patched.

The previous package version (1.5.23-3+deb8u2, DLA-2268-1) provided fixes for the issues referenced above, but they were only applied for the mutt-patched package build, not for the (vanilla) mutt package build.

For Debian 8 'Jessie', this problem has been fixed in version 1.5.23-3+deb8u3.

We recommend that you upgrade your mutt 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/2020/06/msg00040.html
https://packages.debian.org/source/jessie/mutt

Solution

Upgrade the affected mutt, mutt-dbg, and mutt-patched packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (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:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-14093
CVE	CVE-2020-14954

Plugin Information

Published: 2020/07/01, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : mutt_1.5.23-3+deb8u1
Should be : mutt_1.5.23-3+deb8u3
```

138561 - MySQL Denial of Service (Jul 2020 CPU) -

Synopsis

The remote database server is affected by a denial of service vulnerability.

Description

The version of MySQL running on the remote host is 5.7.29 and prior or 8.0.19 and prior. It is, therefore, affected by a vulnerability, as noted in the July 2020 Critical Patch Update advisory:

A Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

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

See Also

http://www.nessus.org/u?dc7b9bd1

Solution

Refer to the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

STIG Severity

I

References

CVE	CVE-2020-14567
XREF	IAVA:2020-A-0321-S

Plugin Information

Published: 2020/07/16, Modified: 2023/11/01

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.62-0+deb8u1
Fixed version : 5.7.30
```

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
```

134220 - nginx < 1.17.7 Information Disclosure -

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

See Also

http://www.nessus.org/u?fd026623

Solution

Upgrade to nginx version 1.17.7 or later.

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

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)

STIG Severity

I

References

CVE	CVE-2019-20372
XREF	IAVB:2020-B-0013-S

Plugin Information

Published: 2020/03/05, Modified: 2024/03/25

Plugin Output

tcp/0

```
Path : nginx (via package manager)
Installed version : 1.6.2-5
Fixed version : 1.17.7
```

125926 - Debian DLA-1818-1 : dbus security update -

Synopsis

The remote Debian host is missing a security 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.

For Debian 8 'Jessie', this problem has been fixed in version 1.8.22-0+deb8u2.

We recommend that you upgrade your dbus 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/2019/06/msg00005.html
https://packages.debian.org/source/jessie/dbus

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

Plugin Information

Published: 2019/06/17, Modified: 2024/05/16

Plugin Output

tcp/0

```
Remote package installed : dbus_1.8.22-0+deb8u1
Should be : dbus_1.8.22-0+deb8u2
Remote package installed : libdbus-1-3_1.8.22-0+deb8u1
Should be : libdbus-1-3_1.8.22-0+deb8u2
```

129305 - Debian DLA-1931-2 : libgcrypt20 regression update -

Synopsis

The remote Debian host is missing a security update.

Description

It was discovered that the fix to address an ECDSA timing attack in the libgcrypt20 cryptographic library was incomplete.

For Debian 8 'Jessie', this issue has been fixed in libgcrypt20 version 1.6.3-2+deb8u8. Thanks to Albert Chin-A-Young <china@thewrittenword.com> for the report.

We recommend that you upgrade your libgcrypt20 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/2020/01/msg00001.html
https://packages.debian.org/source/jessie/libgcrypt20

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2019-13627

Plugin Information

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

Plugin Output

tcp/0

```
Remote package installed : libgcrypt20_1.6.3-2+deb8u5
Should be : libgcrypt20_1.6.3-2+deb8u8
```

130918 - Debian DLA-1989-1 : 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 leak.

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) are listed at <https://en.wikipedia.org/wiki/List_of_Intel_graphics_proces sing_units#Gen8>;.

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 a future DLA. 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 <https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/ tsx_async_abort.html> or in the linux-doc-3.16 package.

Intel's explanation of the issue can be found at <https://software.intel.com/security-software-guidance/insig hts/deep-dive-intel-transactional-synchronization-extensions
-intel-tsx-asynchronous-abort>;.

For Debian 8 'Jessie', these problems have been fixed in version 3.16.76-1. This update also includes other fixes from upstream stable updates.

We recommend that you upgrade your linux 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

http://www.nessus.org/u?aac5629f
https://lists.debian.org/debian-lts-announce/2019/11/msg00009.html
https://packages.debian.org/source/jessie/linux
http://www.nessus.org/u?900f812f
http://www.nessus.org/u?f68ddac1

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-0154

CVE CVE-2019-11135

Plugin Information

Published: 2019/11/13, Modified: 2021/01/11

Plugin Output

tcp/0

```
Remote package installed : linux-image-3.16.0-4-amd64_3.16.51-2
Should be : linux-image-3.16.0-<ANY>-amd64_3.16.76-1
Remote package installed : linux-libc-dev_3.16.64-2
Should be : linux-libc-dev_3.16.76-1

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.
```

131291 - Debian DLA-2006-1 : libxdmcp security update -

Synopsis

The remote Debian host is missing a security update.

Description

It has been found, that libxdmcp, an X11 Display Manager Control Protocol library, uses weak entropy to generate keys.

Using arc4random_buf() from libbsd should avoid this flaw.

For Debian 8 'Jessie', this problem has been fixed in version 1:1.1.1-1+deb8u1.

We recommend that you upgrade your libxdmcp 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/2019/11/msg00024.html
https://packages.debian.org/source/jessie/libxdmcp

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2017-2625

Plugin Information

Published: 2019/11/26, Modified: 2024/04/09

Plugin Output

tcp/0

```
Remote package installed : libxdmcp6_1:1.1.1-1+b1
Should be : libxdmcp6_1:1.1.1-1+deb8u1
```

133219 - Debian DLA-2074-1 : python-apt security update -

Synopsis

The remote Debian host is missing a security update.

Description

Several issues have been found in python-apt, a python interface to libapt-pkg.

CVE-2019-15795

It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages.

CVE-2019-15796

It was discovered that python-apt could install packages from untrusted repositories, contrary to expectations.

For Debian 8 'Jessie', these problems have been fixed in version 0.9.3.13.

We recommend that you upgrade your python-apt 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/2020/01/msg00020.html
https://packages.debian.org/source/jessie/python-apt

Solution

Upgrade the affected packages.

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

Plugin Information

Published: 2020/01/24, Modified: 2024/03/29

Plugin Output

tcp/0

```
Remote package installed : python-apt_0.9.3.12
Should be : python-apt_0.9.3.13
```

```
Remote package installed : python-apt-common_0.9.3.12
Should be : python-apt-common_0.9.3.13
```

136893 - Debian DLA-2221-1 : sqlite3 -

Synopsis

The remote Debian host is missing a security update.

Description

An integer overflow vulnerability was found in the sqlite3_str_vappendf function of the src/printf.c file of sqlite3 from version 3.8.3.

For Debian 8 'Jessie', this problem has been fixed in version 3.8.7.1-1+deb8u6.

We recommend that you upgrade your sqlite3 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/2020/05/msg00024.html
https://packages.debian.org/source/jessie/sqlite3

Solution

Upgrade the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/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:POC/RL:OF/RC:C)

References

CVE CVE-2020-13434

Plugin Information

Published: 2020/05/27, Modified: 2024/03/08

Plugin Output

tcp/0

```
Remote package installed : libsqlite3-0_3.8.7.1-1+deb8u4
Should be : libsqlite3-0_3.8.7.1-1+deb8u6
```

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 difference between the local and remote clocks is 13 seconds.
```

156000 - Apache Log4j Installed (Linux / Unix) -

Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

Note, this plugin runs certain commands differently if the scan is configured to use the 'Attempt Least Privilege' option. If enabled, scan times are expected to increase, especially on hosts with many files.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://logging.apache.org/log4j/2.x/

Solution

n/a

Risk Factor

None

References

XREF	IAVA:0001-A-0650
XREF	IAVT:0001-T-0941

Plugin Information

Published: 2021/12/10, Modified: 2025/08/18

Plugin Output

tcp/0

```
Path : /usr/share/java/libintl.jar
Version : unknown
JMSAppender.class association : Not Found
JdbcAppender.class association : Not Found
JndiLookup.class association : Not Found
Method : Embedded string inspection
```

```
Note: Jar file inspection cannot be performed. No results or cannot list archive contents. If results are present, install an unzip
package to resolve this problem.
```

34098 - BIOS Info (SSH) -

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version : 1.2
Vendor : innotek GmbH
Release Date : 12/01/2006
Secure boot : disabled
```

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:debian:debian_linux:8 -> Debian Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:log4j -> Apache Software Foundation log4j
cpe:/a:gnupg:libgcrypt:1.6.3 -> GnuPG Libgcrypt
cpe:/a:haxx:libcurl:7.38.0 -> Haxx libcurl
cpe:/a:igor_sysoev:nginx:1.6.2 -> Nginx
cpe:/a:mysql:mysql:5.5.62-0%2bdeb8u1_ -> MySQL MySQL
cpe:/a:nginx:nginx:1.6.2 -> Nginx
cpe:/a:nginx:nginx:1.6.2-5 -> Nginx
cpe:/a:openbsd:openssh:6.7 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:6.7p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1t -> OpenSSL Project OpenSSL
cpe:/a:php:php:5.6.40 -> PHP PHP
cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ
cpe:/a:vim:vim:7.4 -> Vim
```

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-5
dc-5 (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)
- 10.50.41.35 (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)
- 2409:40c0:1027:8ebc:a00:27ff:fe23:f7da (on interface eth0)
- fe80::a00:27ff:fe23:f7da (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 :

- 08:00:27:23:f7:da (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 : 08:00:27:23:f7:da
IPv4:
- Address : 10.50.41.35
Netmask : 255.255.255.0
Broadcast : 10.50.41.255
IPv6:
- Address : 2409:40c0:1027:8ebc:a00:27ff:fe23:f7da
Prefixlen : 64
Scope : global
- Address : fe80::a00:27ff:fe23:f7da
Prefixlen : 64
Scope : link
```

179200 - Enumerate the Network Routing configuration via SSH -

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Gateway Routes:
eth0:
ipv4_gateways:
10.50.41.114:
subnets:
- 0.0.0.0/0
ipv6_gateways:
fe80::4a2:97ff:fec8:6a88:
subnets:
- ::/0
Interface Routes:
eth0:
ipv4_subnets:
- 10.50.41.0/24
ipv6_subnets:
- 2409:40c0:1027:8ebc::/64
- fe80::/64
```

168980 - Enumerate the PATH Variables -

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/usr/local/bin
/usr/bin
/bin
/usr/games
```

35716 - Ethernet Card Manufacturer Detection -

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:23:F7:DA : 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:
- 08:00:27:23:F7:DA
```

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 :

nginx/1.6.2
```

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 : no
Options allowed : (Not implemented)
Headers :

Server: nginx/1.6.2
Date: Sat, 08 Nov 2025 18:44:38 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

Response Body :

<!doctype html>

<html lang="en">
```

```
<head>
<meta charset="utf-8">
<title>Welcome</title>
<link rel="stylesheet" href="css/styles.css">
</head>

<body>
<div class="body-wrapper">
<div class="header-wrapper">
<header>
DC-5 is alive!
</header>
</div>

<div class="menu-wrapper">
<menu>
<ul>
<a href="index.php"><li>Home</li></a>
<a href="solutions.php"><li>Solutions</li></a>
<a href="about-us.php"><li>About Us</li></a>
<a href="faq.php"><li>FAQ</li></a>
<a href="contact.php"><li>Contact</li></a>
</ul>
</menu>
</div>

<div class="body-content">
<h2>Welcome</h2>

<p>Cras et dolor a nibh malesuada sagittis sit amet nec ligula. Mauris vitae velit magna. Proin sodales, dolor vel volutpat dapibus, turpis urna malesuada diam, ac pulvinar orci neque quis elit. Integer sollicitudin diam ut dolor tempus ullamcorper. Proin ultrices elit tellus, non finibus felis dignissim in. Aliquam erat volutpat. Quisque a diam ut eros aliquam scelerisque eu ac odio. Etiam dignissim malesuada pulvinar. Suspendisse ullamcorper turpis quis velit tempor, quis venenatis metus iaculis. Mauris mollis risus a turpis vulputate dignissim volutpat eu justo. Nulla aliquam orci id massa semper tempor. Ut dapibus sagittis libero vitae venenatis.

<p>Proin dapibus convallis eleifend. Donec venenatis leo arcu. Donec accumsan erat a massa imperdiet mollis. Curabitur consectetur ac lorem tempor egestas. Integer a quam pharetra, ultricies ipsum non, sodales risus. Aliquam venenatis porta ipsum, porttitor bibendum libero tristique quis. Duis a leo vulputate, sollicitudin lectus vel, pulvinar risus.

<p>Quisque lorem purus, accumsan consectetur pretium sit amet, elementum ac nunc. Etiam at quam sed tellus rutrum lobortis condimentum et nisi. Ut quis malesuada tellus. Integer eget turpis id ligula blandit efficitur eu vel justo. Aenean suscipit ipsum vel venenatis consectetur. Vivamus mattis nulla non commodo lacinia. Aenean ullamcorper dui vel felis porta ullamcorper. Nulla at nunc diam. Donec a porta justo, vitae facilisis erat. Morbi ac rutrum tellus. Vestibulum cursus quam ac elit dictum vehicula. Aenean dapibus sodales nibh id posuere. In hac habitasse platea dictumst. Aliquam facilisis dignissim sodales. Nullam finibus dui nisi, quis scelerisque metus aliquet et. Nam ante libero, sollicitudin eget mauris ac, sollicitudin fermentum odio.

<p>Integer suscipit sodales mi, a bibendum massa rutrum id. Praesent elit lacus, cursus ut turpis nec, tristique semper arcu. Vivamus sed erat vitae tellus pulvinar cursus at in orci. Curabitur massa est, laoreet nec dolor vel, condimentum suscipit erat. Maecenas pulvinar eget est eget porta. Aliquam et eros aliquam, elementum mi eget, faucibus urna. Aliquam hendrerit, nisl id mattis fringilla, nunc lectus cursus leo, non condimentum massa augue ac erat.

<p>Mauris elit lectus, ultrices cursus dapibus quis, tristique sed urna. Sed ultrices sapien et leo sodales lacinia. Interdum et malesuada fames ac ante ipsum primis in faucibus. Fusce nunc mi, gravida tempor molestie eget, fermentum vel justo. Etiam pulvinar tempor risus id aliquam. Vivamus sit amet lobortis enim. Nulla et faucibus arcu, in euismod sem.

<p>Vivamus pharetra in odio quis viverra. Suspendisse non euismod lacus. Donec cursus venenatis erat sit amet rutrum. Aliquam vitae tristique sapien. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nunc eget viverra nisi. Praesent quis condimentum ex. Mauris in lectus sed odio viverra porta vitae eu nisi. Pellentesque dapibus sit amet augue eu semper. Etiam et tortor malesuada, auctor nibh non, cursus dolor. Pellentesque in eros lacus. Sed euismod gravida tristique. Nulla vulputate urna nec nulla vestibulum fermentum. Praesent viverra lectus nibh, at gravida quam sollicitudin et.

</div>

<div class="footer-wrapper">
<footer>
Copyright © 2019
</footer>
</div>
</div>
</body>
</html>
```

171410 - IP Assignment Method Detection -

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ eth0
+ IPv4
- Address : 10.50.41.35
Assign Method : static
+ IPv6
- Address : 2409:40c0:1027:8ebc:a00:27ff:fe23:f7da
Assign Method : dynamic
- Address : fe80::a00:27ff:fe23:f7da
Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX) -

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20.0.3
Version : 1.6.3

Path : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version : 1.6.3
```

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
/dev/sda1 4.6G 1.3G 3.1G 30% /
udev 10M 0 10M 0% /dev
tmpfs 201M 4.4M 196M 3% /run
tmpfs 501M 28K 501M 1% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 501M 0 501M 0% /sys/fs/cgroup


$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 5G 0 disk
├─sda1 8:1 0 4.8G 0 part /
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 259M 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,relatime,size=10240k,nr_inodes=125941,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,relatime,size=204864k,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/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
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/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=22,pgrp=1,timeout=300,minproto=5,maxproto=5,direct)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
rpc_pipefs on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
```

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 : dc
Home folder : /home/dc
Start script : /bin/bash
Groups : video
cdrom
dc
netdev
floppy
plugdev
dip
audio

User : yash
Home folder : /home/yash
Start script : /bin/sh
Groups : sudo
yash

----------[ System Accounts ]----------

User : root
Home folder : /root
Start script : /bin/bash
Groups : root

User : daemon
Home folder : /usr/sbin
Start script : /usr/sbin/nologin
Groups : daemon

User : bin
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : bin

User : sys
Home folder : /dev
Start script : /usr/sbin/nologin
Groups : sys

User : sync
Home folder : /bin
Start script : /bin/sync
Groups : nogroup

User : games
Home folder : /usr/games
Start script : /usr/sbin/nologin
Groups : games

User : man
Home folder : /var/cache/man
Start script : /usr/sbin/nologin
Groups : man

User : lp
Home folder : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups : lp

User : mail
```

```
Home folder : /var/mail
Start script : /usr/sbin/nologin
Groups : mail

User : news
Home folder : /var/spool/news
Start script : /usr/sbin/nologin
Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups : uucp

User : proxy
Home folder : /bin
Start script : /usr/sbin/nologin
Groups : proxy

User : www-data
Home folder : /var/www
Start script : /usr/sbin/nologin
Groups : www-data

User : backup
Home folder : /var/backups
Start script : /usr/sbin/nologin
Groups : backup

User : list
Home folder : /var/list
Start script : /usr/sbin/nologin
Groups : list

User : irc
Home folder : /var/run/ircd
Start script : /usr/sbin/nologin
Groups : irc

User : gnats
Home folder : /var/lib/gnats
Start script : /usr/sbin/nologin
Groups : gnats

User : nobody
Home folder : /nonexistent
Start script : /usr/sbin/nologin
Groups : nogroup

User : systemd-timesync
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-timesync

User : systemd-network
Home folder : /run/systemd/netif
Start script : /bin/false
Groups : systemd-network

User : systemd-resolve
Home folder : /run/systemd/resolve
Start script : /bin/false
Groups : systemd-resolve

User : systemd-bus-proxy
Home folder : /run/systemd
Start script : /bin/false
Groups : systemd-bus-proxy

User : Debian-exim
Home folder : /var/spool/exim4
Start script : /bin/false
Groups : Debian-exim

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : statd
Home folder : /var/lib/nfs
Start script : /bin/false
Groups : nogroup

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql

User : sshd
Home folder : /var/run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup


----------[ Domain Accounts ]----------
```

129468 - MySQL Server Installed (Linux) -

Synopsis

MySQL Server is installed on the remote Linux host.

Description

MySQL Server is installed on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/30, Modified: 2025/04/18

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Version : 5.5.62-0+deb8u1
```

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 - 5
Scan policy used : Advanced Scan
Scanner IP : 10.50.41.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 101.281 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 'yash' 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 : 2025/11/8 18:44 UTC
Scan duration : 383 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
```

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/111/rpc-portmapper

```
Port 111/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/111/rpc-portmapper

```
Port 111/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/999

```
Port 999/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/25192

```
Port 25192/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/36237/rpc-status

```
Port 36237/tcp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/43019

```
Port 43019/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/45962

```
Port 45962/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/49946

```
Port 49946/udp was found to be open
```

14272 - Netstat Portscanner (SSH) -

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

https://en.wikipedia.org/wiki/Netstat

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/50638/rpc-status

```
Port 50638/udp was found to be open
```

209654 - OS Fingerprints Detected -

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 3.16 on Debian 8.0 (jessie)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8

Remote operating system : Linux Kernel 3.16.0-4-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux dc-5 3.16.0-4-amd64 #1 SMP Debian 3.16.51-2 (2017-12-03) x86_64 GNU/Linux


Remote operating system : Linux
Confidence level : 59
```

```
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W29200:O0204ffff:M1460:
P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191303_7_p=22

Remote operating system : Linux Kernel 3.16.0-4-amd64 on Debian 8.10
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
HTTP:!:Server: nginx/1.6.2
```

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 3.16.0-4-amd64 on Debian 8.10
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.16.0-4-amd64 on Debian 8.10
```

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-5 3.16.0-4-amd64 #1 SMP Debian 3.16.51-2 (2017-12-03) x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
8.10

OS Security Patch Assessment is available for this host.
Runtime : 4.711294 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 : yash
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 : 6.7p1
Banner : SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8
```

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 3 installs of OpenSSL:

Path : /usr/bin/openssl
Version : 1.0.1t
Associated Package : openssl 1.0.1t-1
Managed by OS : True

Path : /usr/lib/x86_64-linux-gnu/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0

Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version
within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libatalla.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/x86_64-linux-gnu/openssl-1.0.0/engines/libgmp.so
```

216936 - PHP Scripting Language Installed (Unix) -

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.
Thorough test is required to get results on hosts running MacOS.

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 3 installs of PHP:

Path : /usr/bin/php5
Version : 5.6.40
Associated Package : php5-cli: /usr/bin/php5
INI file : /etc/php5/cli/php.ini
INI source : PHP binary grep
Managed by OS : True

Path : /usr/bin/php5-cgi
Version : 5.6.40
Associated Package : php5-cgi: /usr/bin/php5-cgi
INI file : /etc/php5/cgi/php.ini
INI source : PHP binary grep
Managed by OS : True

Path : /usr/lib/cgi-bin/php5
Version : 5.6.40
Associated Package : php5-cgi: /usr/lib/cgi-bin/php5
INI file : /etc/php5/cgi/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 47 actions :

[ Debian DLA-1828-1 : python-urllib3 security update (126077) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-1839-1 : expat security update (126348) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-1864-1 : patch security update (127076) ]
+ Action to take : Upgrade the affected patch package.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Debian DLA-1866-2 : glib2.0 regression update (127475) ]
+ Action to take : Upgrade the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Debian DLA-1871-1 : vim security update (127480) ]
+ Action to take : Upgrade the affected packages.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[ Debian DLA-1909-1 : freetype security update (128509) ]
+ Action to take : Upgrade the affected packages.
+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[ Debian DLA-1917-1 : curl security update (128777) ]
+ Action to take : Upgrade the affected packages.
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ Debian DLA-1925-1 : python2.7 security update (128883) ]
+ Action to take : Upgrade the affected packages.
+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).

[ Debian DLA-1931-2 : libgcrypt20 regression update (129305) ]
+ Action to take : Upgrade the affected packages.

[ Debian DLA-1932-1 : openssl security update (129362) ]
```

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-1969-1 : file security update (130182)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-1973-1 : libxslt security update (130286)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Debian DLA-1981-1 : cpio security update (130522)]

+ Action to take : Upgrade the affected cpio, and cpio-win32 packages.

[Debian DLA-1991-1 : libssh2 security update (130980)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2003-1 : isc-dhcp security update (131248)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2006-1 : libxdmcp security update (131291)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2009-1 : tiff security update (131328)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Debian DLA-2020-1 : libonig security update (131705)]

+ Action to take : Upgrade the affected libonig-dev, libonig2, and libonig2-dbg packages.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).

[Debian DLA-2040-1 : harfbuzz security update (132107)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2044-1 : cyrus-sasl2 security update (132344)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2048-1 : libxml2 security update (132420)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2052-1 : libbsd security update (132514)]

+ Action to take : Upgrade the affected libbsd-dev, libbsd0, and libbsd0-dbg packages.

[Debian DLA-2074-1 : python-apt security update (133219)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2085-1 : zlib security update (133323)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).

[Debian DLA-2086-1 : wget security update (133324)]

+ Action to take : Upgrade the affected wget package.

[Debian DLA-2106-1 : libgd2 security update (133730)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2136-1 : libvpx security update (134352)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian DLA-2151-1 : icu security update (134768)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2156-1 : e2fsprogs security update (134880)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2195-1 : w3m security update (136204)]

+ Action to take : Upgrade the affected w3m, and w3m-img packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2199-1 : openldap security update (136289)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian DLA-2210-1 : apt security update (136631)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2213-1 : exim4 security update (136702)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2221-1 : sqlite3 (136893)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2227-1 : bind9 security update (136983)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).

[Debian DLA-2228-2 : json-c regression update (136984)]

+ Action to take : Upgrade the affected packages.

[Debian DLA-2235-1 : dbus security update (137205)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[Debian DLA-2237-1 : cups security update (137207)]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

[Debian DLA-2241-2 : linux security update (137283)]

+ Action to take : Upgrade the affected packages.

```
+Impact : Taking this action will resolve 173 different vulnerabilities (CVEs).


[ Debian DLA-2255-1 : libtasn1-6 security update (137858) ]

+ Action to take : Upgrade the affected packages.


[ Debian DLA-2256-1 : libtirpc security update (137859) ]

+ Action to take : Upgrade the affected libtirpc-dev, and libtirpc1 packages.


[ Debian DLA-2261-1 : php5 security update (137886) ]

+ Action to take : Upgrade the affected packages.

+Impact : Taking this action will resolve 20 different vulnerabilities (CVEs).


[ Debian DLA-2268-2 : mutt regression update (137911) ]

+ Action to take : Upgrade the affected mutt, mutt-dbg, and mutt-patched packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Debian DSA-4196-1 : linux - security update (109658) ]

+ Action to take : Upgrade the linux packages.

For the oldstable distribution (jessie), these problems have been fixed in version 3.16.56-1+deb8u1. This update includes various
fixes for regressions from 3.16.56-1 as released in DSA-4187-1 (Cf. #897427, #898067 and #898100).

For the stable distribution (stretch), these problems have been fixed in version 4.9.88-1+deb9u1. The fix for CVE-2018-1108 applied
in DSA-4188-1 is temporarily reverted due to various regression, cf.
#897599.

+Impact : Taking this action will resolve 50 different vulnerabilities (CVEs).


[ MySQL Denial of Service (Jul 2020 CPU) (138561) ]

+ Action to take : Refer to the vendor advisory.


[ 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.


[ nginx < 1.17.7 Information Disclosure (134220) ]

+ Action to take : Upgrade to nginx version 1.17.7 or later.
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :
```

```
- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/36237/rpc-status

```
The following RPC services are available on TCP port 36237 :

- program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/50638/rpc-status

```
The following RPC services are available on UDP port 50638 :

- program: 100024 (status), version: 1
```

53335 - RPC portmapper (TCP) -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

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 :
- 2409:40c0:1027:8ebc:a00:27ff:fe23:f7da
```

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
ssh-dss
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for kex_algorithms :

curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

102094 - SSH Commands Require Privilege Escalation -

Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0507

Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

Plugin Output

tcp/0

```
Login account : yash
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 : "strings '/var/log/apache2' 2>&1"
Response : "strings: /var/log/apache2: Permission denied"
Error : "\nCould not chdir to home directory /home/yash: No such file or directory"
- Command : "strings '/var/log/apache2' 2>&1"
Response : "strings: /var/log/apache2: Permission denied"
Error : "\nCould not chdir to home directory /home/yash: No such file or directory"
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 2.12"
Error : "\nCould not chdir to home directory /home/yash: No such file or directory\n\n/dev/mem: Permission denied"
- Plugin Filename : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
- Command : "/usr/sbin/dmidecode -s system-version 2>&1"
Response : "/dev/mem: Permission denied"
Error : "\nCould not chdir to home directory /home/yash: No such file or directory"
- 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 : "/dev/mem: Permission denied"
Error : "\nCould not chdir to home directory /home/yash: No such file or directory"
- 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 : "\nCould not chdir to home directory /home/yash: No such file or directory\n\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 : "\nCould not chdir to home directory /home/yash: No such file or directory\n\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 : "\nCould not chdir to home directory /home/yash: No such file or directory\n\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 : "\nCould not chdir to home directory /home/yash: No such file or directory\n\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
```

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_6.7p1 Debian-5+deb8u8
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/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22869 - Software Enumeration (SSH) -

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

ii acl 2.2.52-2 amd64 Access control list utilities
ii acpi 1.7-1 amd64 displays information on ACPI devices
ii acpi-support-base 0.142-6 all scripts for handling base ACPI events such as the power button
ii acpid 1:2.0.23-2 amd64 Advanced Configuration and Power Interface event daemon
ii adduser 3.113+nmu3 all add and remove users and groups
rc apache2 2.4.10-10+deb8u14 amd64 Apache HTTP Server
rc apache2-bin 2.4.10-10+deb8u14 amd64 Apache HTTP Server (modules and other binary files)
ii apt 1.0.9.8.5 amd64 commandline package manager
ii apt-listchanges 2.85.13+nmu1 all package change history notification tool
ii apt-utils 1.0.9.8.5 amd64 package management related utility programs
ii aptitude 0.6.11-1+b1 amd64 terminal-based package manager
ii aptitude-common 0.6.11-1 all architecture independent files for the aptitude package manager
ii aptitude-doc-en 0.6.11-1 all English manual for aptitude, a terminal-based package manager
ii at 3.1.16-1 amd64 Delayed job execution and batch processing
ii base-files 8+deb8u10 amd64 Debian base system miscellaneous files
ii base-passwd 3.5.37 amd64 Debian base system master password and group files
ii bash 4.3-11+deb8u2 amd64 GNU Bourne Again SHell
ii bash-completion 1:2.1-4 all programmable completion for the bash shell
ii bc 1.06.95-9 amd64 GNU bc arbitrary precision calculator language
ii bind9-host 1:9.9.5.dfsg-9+deb8u17 amd64 Version of 'host' bundled with BIND 9.X
ii binutils 2.25-5+deb8u1 amd64 GNU assembler, linker and binary utilities
ii bsd-mailx 8.1.2-0.20141216cvs-2 amd64 simple mail user agent
ii bsdmainutils 9.0.6 amd64 collection of more utilities from FreeBSD
ii bsdutils 1:2.25.2-6 amd64 basic utilities from 4.4BSD-Lite
ii build-essential 11.7 amd64 Informational list of build-essential packages
ii busybox 1:1.22.0-9+deb8u4 amd64 Tiny utilities for small and embedded systems
ii bzip2 1.0.6-7+b3 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20141019+deb8u4 all Common CA certificates
ii console-setup 1.123 all console font and keymap setup program
ii console-setup-linux 1.123 all Linux specific part of console-setup
ii coreutils 8.23-4 amd64 GNU core utilities
ii cpio 2.11+dfsg-4.1+deb8u1 amd64 GNU cpio -- a program to manage archives of files
ii cpp 4:4.9.2-2 amd64 GNU C preprocessor (cpp)
```

```
ii cpp-4.9 4.9.2-10+deb8u2 amd64 GNU C preprocessor
ii cron 3.0pl1-127+deb8u2 amd64 process scheduling daemon
ii dash 0.5.7-4+b1 amd64 POSIX-compliant shell
ii dbus 1.8.22-0+deb8u1 amd64 simple interprocess messaging system (daemon and utilities)
ii dc 1.06.95-9 amd64 GNU dc arbitrary precision reverse-polish calculator
ii debconf 1.5.56+deb8u1 all Debian configuration management system
ii debconf-i18n 1.5.56+deb8u1 all full internationalization support for debconf
ii debian-archive-keyring 2017.5~deb8u1 all GnuPG archive keys of the Debian archive
ii debian-faq 5.0.3 all Debian Frequently Asked Questions
ii debianutils 4.4+b1 amd64 Miscellaneous utilities specific to Debian
ii dictionaries-common 1.23.17 all spelling dictionaries - common utilities
ii diffutils 1:3.3-1+b1 amd64 File comparison utilities
ii discover 2.1.2-7 amd64 hardware identification system
ii discover-data 2.2013.01.11 all Data lists for Discover hardware detection system
ii dmidecode 2.12-3 amd64 SMBIOS/DMI table decoder
ii dmsetup 2:1.02.90-2.2+deb8u1 amd64 Linux Kernel Device Mapper userspace library
ii dnsutils 1:9.9.5.dfsg-9+deb8u17 amd64 Clients provided with BIND
ii doc-debian 6.2 all Debian Project documentation and other documents
ii docutils-common 0.12+dfsg-1 all text processing system for reStructuredText - common data
ii docutils-doc 0.12+dfsg-1 all text processing system for reStructuredText - documentation
ii dpkg 1.17.27 amd64 Debian package management system
ii dpkg-dev 1.17.27 all Debian package development tools
ii e2fslibs 1.42.12-2+b1 amd64 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.42.12-2+b1 amd64 ext2/ext3/ext4 file system utilities
ii eject 2.1.5+deb1+cvs20081104-13.1+deb8u1 amd64 ejects CDs and operates CD-Changers under Linux
ii emacsen-common 2.0.8 all Common facilities for all emacsen
ii exim4 4.84.2-2+deb8u5 all metapackage to ease Exim MTA (v4) installation
ii exim4-base 4.84.2-2+deb8u5 amd64 support files for all Exim MTA (v4) packages
ii exim4-config 4.84.2-2+deb8u5 all configuration for the Exim MTA (v4)
ii exim4-daemon-light 4.84.2-2+deb8u5 amd64 lightweight Exim MTA (v4) daemon
ii fakeroot 1.20.2-1 amd64 tool for simulating superuser privileges
ii file 1:5.22+15-2+deb8u5 amd64 Determines file type using "magic" numbers
ii findutils 4.4.2-9+b1 amd64 utilities for finding files--find, xargs
ii fontconfig 2.11.0-6.3+deb8u1 amd64 generic font configuration library - support binaries
ii fontconfig-config 2.11.0-6.3+deb8u1 all generic font configuration library - configuration
ii fonts-dejavu-core 2.34-1 all Vera font family derivate with additional characters
ii ftp 0.17-31 amd64 classical file transfer client
ii g++ 4:4.9.2-2 amd64 GNU C++ compiler
ii g++-4.9 4.9.2-10+deb8u2 amd64 GNU C++ compiler
ii gcc 4:4.9.2-2 amd64 GNU C compiler
ii gcc-4.8-base 4.8.4-1 amd64 GCC, the GNU Compiler Collection (base package)
ii gcc-4.9 4.9.2-10+deb8u2 amd64 GNU C compiler
ii gcc-4.9-base 4.9.2-10+deb8u2 amd64 GCC, the GNU Compiler Collection (base package)
ii geoip-database 20150317-1 all IP lookup command line tools that use the GeoIP library (country database)
ii gettext-base 0.19.3-2 amd64 GNU Internationalization utilities for the base system
ii gnupg 1.4.18-7+deb8u5 amd64 GNU privacy guard - a free PGP replacement
ii gnupg-agent 2.0.26-6+deb8u2 amd64 GNU privacy guard - password agent
ii gnupg2 2.0.26-6+deb8u2 amd64 GNU privacy guard - a free PGP replacement (new v2.x)
ii gpgv 1.4.18-7+deb8u5 amd64 GNU privacy guard - signature verification tool
ii grep 2.20-4.1 amd64 GNU grep, egrep and fgrep
ii groff-base 1.22.2-8 amd64 GNU troff text-formatting system (base system components)
ii grub-common 2.02~beta2-22+deb8u1 amd64 GRand Unified Bootloader (common files)
ii grub-pc 2.02~beta2-22+deb8u1 amd64 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 2.02~beta2-22+deb8u1 amd64 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
ii grub2-common 2.02~beta2-22+deb8u1 amd64 GRand Unified Bootloader (common files for version 2)
ii gzip 1.6-4 amd64 GNU compression utilities
ii hicolor-icon-theme 0.13-1 all default fallback theme for FreeDesktop.org icon themes
ii host 1:9.9.5.dfsg-9+deb8u17 all Transitional package
ii hostname 3.15 amd64 utility to set/show the host name or domain name
ii iamerican 3.3.02-6 all American English dictionary for ispell (standard version)
ii ibritish 3.3.02-6 all British English dictionary for ispell (standard version)
ii ienglish-common 3.3.02-6 all Common files for British and American ispell dictionaries
ii ifupdown 0.7.53.1 amd64 high level tools to configure network interfaces
ii info 5.2.0.dfsg.1-6 amd64 Standalone GNU Info documentation browser
ii init 1.22 amd64 System-V-like init utilities - metapackage
ii init-system-helpers 1.22 all helper tools for all init systems
ii initramfs-tools 0.120+deb8u3 all generic modular initramfs generator
ii initscripts 2.88dsf-59 amd64 scripts for initializing and shutting down the system
ii insserv 1.14.0-5 amd64 boot sequence organizer using LSB init.d script dependency information
ii install-info 5.2.0.dfsg.1-6 amd64 Manage installed documentation in info format
ii installation-report 2.58 all system installation report
ii iproute2 3.16.0-2 amd64 networking and traffic control tools
ii iptables 1.4.21-2+b1 amd64 administration tools for packet filtering and NAT
ii iputils-ping 3:20121221-5+b2 amd64 Tools to test the reachability of network hosts
ii isc-dhcp-client 4.3.1-6+deb8u3 amd64 DHCP client for automatically obtaining an IP address
ii isc-dhcp-common 4.3.1-6+deb8u3 amd64 common files used by all of the isc-dhcp packages
ii iso-codes 3.57-1 all ISO language, territory, currency, script codes and their translations
ii ispell 3.3.02-6 amd64 International Ispell (an interactive spelling corrector)
ii kbd 1.15.5-2 amd64 Linux console font and keytable utilities
ii keyboard-configuration 1.123 all system-wide keyboard preferences
ii klibc-utils 2.0.4-2 amd64 small utilities built with klibc for early boot
ii kmod 18-3 amd64 tools for managing Linux kernel modules
ii krb5-locales 1.12.1+dfsg-19+deb8u5 all Internationalization support for MIT Kerberos
ii laptop-detect 0.13.7 amd64 attempt to detect a laptop
ii less 458-3 amd64 pager program similar to more
ii libacl1 2.2.52-2 amd64 Access control list shared library
ii libaio1 0.3.110-1 amd64 Linux kernel AIO access library - shared library
ii libalgorithm-c3-perl 0.09-1 all Perl module for merging hierarchies using the C3 algorithm
ii libalgorithm-diff-perl 1.19.02-3 all module to find differences between files
ii libalgorithm-diff-xs-perl 0.04-3+b1 amd64 module to find differences between files (XS accelerated)
ii libalgorithm-merge-perl 0.08-2 all Perl module for three-way merge of textual data
rc libapache2-mod-php5 5.6.40+dfsg-0+deb8u2 amd64 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapparmor1 2.9.0-3 amd64 changehat AppArmor library
rc libapr1 1.5.1-3 amd64 Apache Portable Runtime Library
rc libaprutil1 1.5.4-1 amd64 Apache Portable Runtime Utility Library
ii libapt-inst1.5 1.0.9.8.5 amd64 deb package format runtime library
ii libapt-pkg4.12 1.0.9.8.5 amd64 package management runtime library
ii libarchive-extract-perl 0.72-1 all generic archive extracting module
ii libasan1 4.9.2-10+deb8u2 amd64 AddressSanitizer -- a fast memory error detector
```

```
ii libasprintf0c2 0.19.3-2 amd64 GNU library to use fprintf and friends in C++
ii libassuan0 2.1.2-2 amd64 IPC library for the GnuPG components
ii libatk1.0-0 2.14.0-1 amd64 ATK accessibility toolkit
ii libatk1.0-data 2.14.0-1 all Common files for the ATK accessibility toolkit
ii libatomic1 4.9.2-10+deb8u2 amd64 support library providing __atomic built-in functions
ii libattr1 1:2.4.47-2 amd64 Extended attribute shared library
ii libaudit-common 1:2.4-1 all Dynamic library for security auditing - common files
ii libaudit1 1:2.4-1+b1 amd64 Dynamic library for security auditing
ii libauthen-sasl-perl 2.1600-1 all Authen::SASL - SASL Authentication framework
ii libavahi-client3 0.6.31-5 amd64 Avahi client library
ii libavahi-common-data 0.6.31-5 amd64 Avahi common data files
ii libavahi-common3 0.6.31-5 amd64 Avahi common library
ii libbind9-90 1:9.9.5.dfsg-9+deb8u17 amd64 BIND9 Shared Library used by BIND
ii libblkid1 2.25.2-6 amd64 block device id library
ii libboost-iostreams1.55.0 1.55.0+dfsg-3 amd64 Boost.Iostreams Library
ii libbsd0 0.7.0-2 amd64 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-7+b3 amd64 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.19-18+deb8u10 amd64 GNU C Library: Binaries
ii libc-dev-bin 2.19-18+deb8u10 amd64 GNU C Library: Development binaries
ii libc6 2.19-18+deb8u10 amd64 GNU C Library: Shared libraries
ii libc6-dev 2.19-18+deb8u10 amd64 GNU C Library: Development Libraries and Header Files
ii libcairo2 1.14.0-2.1+deb8u2 amd64 Cairo 2D vector graphics library
ii libcap-ng0 0.7.4-2 amd64 An alternate POSIX capabilities library
ii libcap2 1:2.24-8 amd64 POSIX 1003.1e capabilities (library)
ii libcap2-bin 1:2.24-8 amd64 POSIX 1003.1e capabilities (utilities)
ii libcgi-fast-perl 1:2.04-1 all CGI subclass for work with FCGI
ii libcgi-pm-perl 4.09-1 all module for Common Gateway Interface applications
ii libcilkrts5 4.9.2-10+deb8u2 amd64 Intel Cilk Plus language extensions (runtime)
ii libclass-accessor-perl 0.34-1 all Perl module that automatically generates accessors
ii libclass-c3-perl 0.26-1 all pragma for using the C3 method resolution order
ii libclass-c3-xs-perl 0.13-2+b1 amd64 Perl module to accelerate Class::C3
ii libclass-isa-perl 0.36-5 all report the search path for a class's ISA tree
ii libcloog-isl4 0.18.2-1+b2 amd64 Chunky Loop Generator (runtime library)
ii libcomerr2 1.42.12-2+b1 amd64 common error description library
ii libcpan-meta-perl 2.142690-1 all Perl module to access CPAN distributions metadata
ii libcryptsetup4 2:1.6.6-5 amd64 disk encryption support - shared library
ii libcups2 1.7.5-11+deb8u4 amd64 Common UNIX Printing System(tm) - Core library
ii libcurl3-gnutls 7.38.0-4+deb8u14 amd64 easy-to-use client-side URL transfer library (GnuTLS flavour)
ii libcwidget3 0.5.17-2 amd64 high-level terminal interface library for C++ (runtime files)
ii libdata-optlist-perl 0.109-1 all module to parse and validate simple name/value option pairs
ii libdata-section-perl 0.200006-1 all module to read chunks of data from a module's DATA section
ii libdatrie1 0.2.8-1 amd64 Double-array trie library
ii libdb5.3 5.3.28-9+deb8u1 amd64 Berkeley v5.3 Database Libraries [runtime]
ii libdbd-mysql-perl 4.028-2+deb8u2 amd64 Perl5 database interface to the MySQL database
ii libdbi-perl 1.631-3+b1 amd64 Perl Database Interface (DBI)
ii libdbus-1-3 1.8.22-0+deb8u1 amd64 simple interprocess messaging system (library)
ii libdebconfclient0 0.192 amd64 Debian Configuration Management System (C-implementation library)
ii libdevmapper1.02.1 2:1.02.90-2.2+deb8u1 amd64 Linux Kernel Device Mapper userspace library
ii libdiscover2 2.1.2-7 amd64 hardware identification library
ii libdns-export100 1:9.9.5.dfsg-9+deb8u17 amd64 Exported DNS Shared Library
ii libdns100 1:9.9.5.dfsg-9+deb8u17 amd64 DNS Shared Library used by BIND
ii libdpkg-perl 1.17.27 all Dpkg perl modules
ii libedit2 3.1-20140620-2 amd64 BSD editline and history libraries
ii libencode-locale-perl 1.03-1 all utility to determine the locale encoding
ii libestr0 0.1.9-1.1 amd64 Helper functions for handling strings (lib)
ii libevent-2.0-5 2.0.21-stable-2+deb8u1 amd64 Asynchronous event notification library
ii libexpat1 2.1.0-6+deb8u4 amd64 XML parsing C library - runtime library
ii libfakeroot 1.20.2-1 amd64 tool for simulating superuser privileges - shared libraries
ii libfcgi-perl 0.77-1+deb8u1 amd64 helper module for FastCGI
ii libffi6 3.1-2+deb8u1 amd64 Foreign Function Interface library runtime
ii libfile-fcntllock-perl 0.22-1+b1 amd64 Perl module for file locking with fcntl(2)
ii libfile-listing-perl 6.04-1 all module to parse directory listings
ii libfont-afm-perl 1.20-1 all Font::AFM - Interface to Adobe Font Metrics files
ii libfontconfig1 2.11.0-6.3+deb8u1 amd64 generic font configuration library - runtime
ii libfreetype6 2.5.2-3+deb8u2 amd64 FreeType 2 font engine, shared library files
ii libfuse2 2.9.3-15+deb8u3 amd64 Filesystem in Userspace (library)
ii libgc1c2 1:7.2d-6.4 amd64 conservative garbage collector for C and C++
ii libgcc-4.9-dev 4.9.2-10+deb8u2 amd64 GCC support library (development files)
ii libgcc1 1:4.9.2-10+deb8u2 amd64 GCC support library
ii libgcrypt20 1.6.3-2+deb8u5 amd64 LGPL Crypto library - runtime library
ii libgd3 2.1.0-5+deb8u12 amd64 GD Graphics Library
ii libgdbm3 1.8.3-13.1 amd64 GNU dbm database routines (runtime version)
ii libgdk-pixbuf2.0-0 2.31.1-2+deb8u7 amd64 GDK Pixbuf library
ii libgdk-pixbuf2.0-common 2.31.1-2+deb8u7 all GDK Pixbuf library - data files
ii libgeoip1 1.6.2-4 amd64 non-DNS IP-to-country resolver library
ii libglib2.0-0 2.42.1-1+b1 amd64 GLib library of C routines
ii libglib2.0-data 2.42.1-1 all Common files for GLib library
ii libgmp10 2:6.0.0+dfsg-6 amd64 Multiprecision arithmetic library
ii libgnutls-deb0-28 3.3.30-0+deb8u1 amd64 GNU TLS library - main runtime library
ii libgnutls-openssl27 3.3.30-0+deb8u1 amd64 GNU TLS library - OpenSSL wrapper
ii libgomp1 4.9.2-10+deb8u2 amd64 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.17-3 amd64 library for common error values and messages in GnuPG components
ii libgpgme11 1.5.1-6 amd64 GPGME - GnuPG Made Easy (library)
ii libgpm2 1.20.4-6.1+b2 amd64 General Purpose Mouse - shared library
ii libgraphite2-3 1.3.10-1~deb8u1 amd64 Font rendering engine for Complex Scripts -- library
ii libgssapi-krb5-2 1.12.1+dfsg-19+deb8u5 amd64 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgtk2.0-0 2.24.25-3+deb8u2 amd64 GTK+ graphical user interface library
ii libgtk2.0-bin 2.24.25-3+deb8u2 amd64 programs for the GTK+ graphical user interface library
ii libgtk2.0-common 2.24.25-3+deb8u2 all common files for the GTK+ graphical user interface library
ii libharfbuzz0b 0.9.35-2 amd64 OpenType text shaping engine (shared library)
ii libhogweed2 2.7.1-5+deb8u2 amd64 low level cryptographic library (public-key cryptos)
ii libhtml-form-perl 6.03-1 all module that represents an HTML form element
ii libhtml-format-perl 2.11-1 all module for transforming HTML into various formats
ii libhtml-parser-perl 3.71-1+b3 amd64 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-2 all Data tables pertaining to HTML
ii libhtml-template-perl 2.95-1 all module for using HTML templates with Perl
ii libhtml-tree-perl 5.03-1 all Perl module to represent and create HTML syntax trees
ii libhttp-cookies-perl 6.01-1 all HTTP cookie jars
ii libhttp-daemon-perl 6.01-1 all simple http server class
```

```
ii libhttp-date-perl 6.02-1 all module of date conversion routines
ii libhttp-message-perl 6.06-1 all perl interface to HTTP style messages
ii libhttp-negotiate-perl 6.00-2 all implementation of content negotiation
ii libicu52 52.1-8+deb8u7 amd64 International Components for Unicode
ii libidn11 1.29-1+deb8u3 amd64 GNU Libidn library, implementation of IETF IDN specifications
ii libintl-perl 1.23-1+deb8u1 all Uniforum message translations system compatible i18n library
ii libio-html-perl 1.001-1 all open an HTML file with automatic charset detection
ii libio-socket-ip-perl 0.32-1 all module for using IPv4 and IPv6 sockets in a protocol-independent way
ii libio-socket-ssl-perl 2.002-2+deb8u3 all Perl module implementing object oriented interface to SSL sockets
ii libio-string-perl 1.08-3 all Emulate IO::File interface for in-core strings
ii libirs-export91 1:9.9.5.dfsg-9+deb8u17 amd64 Exported IRS Shared Library
ii libisc-export95 1:9.9.5.dfsg-9+deb8u17 amd64 Exported ISC Shared Library
ii libisc95 1:9.9.5.dfsg-9+deb8u17 amd64 ISC Shared Library used by BIND
ii libisccc90 1:9.9.5.dfsg-9+deb8u17 amd64 Command Channel Library used by BIND
ii libisccfg-export90 1:9.9.5.dfsg-9+deb8u17 amd64 Exported ISC CFG Shared Library
ii libisccfg90 1:9.9.5.dfsg-9+deb8u17 amd64 Config File Handling Library used by BIND
ii libisl10 0.12.2-2 amd64 manipulating sets and relations of integer points bounded by linear constraints
ii libitm1 4.9.2-10+deb8u2 amd64 GNU Transactional Memory Library
ii libjasper1 1.900.1-debian1-2.4+deb8u6 amd64 JasPer JPEG-2000 runtime library
ii libjbig0 2.1-3.1 amd64 JBIGkit libraries
ii libjpeg62-turbo 1:1.3.1-12+deb8u2 amd64 libjpeg-turbo JPEG runtime library
ii libjson-c2 0.11-4 amd64 JSON manipulation library - shared library
ii libk5crypto3 1.12.1+dfsg-19+deb8u5 amd64 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.9-5+b1 amd64 Linux Key Management Utilities (library)
ii libklibc 2.0.4-2 amd64 minimal libc subset for use with initramfs
ii libkmod2 18-3 amd64 libkmod shared library
ii libkrb5-3 1.12.1+dfsg-19+deb8u5 amd64 MIT Kerberos runtime libraries
ii libkrb5support0 1.12.1+dfsg-19+deb8u5 amd64 MIT Kerberos runtime libraries - Support library
ii libksba8 1.3.2-1+deb8u1 amd64 X.509 and CMS support library
ii liblcms2-2 2.6-3+deb8u2 amd64 Little CMS 2 color management library
ii libldap-2.4-2 2.4.40+dfsg-1+deb8u3 amd64 OpenLDAP libraries
ii liblocale-gettext-perl 1.05-8+b1 amd64 module using libc functions for internationalization in Perl
ii liblockfile-bin 1.09-6 amd64 support binaries for and cli utilities based on liblockfile
ii liblockfile1 1.09-6 amd64 NFS-safe locking library
ii liblog-message-perl 0.8-1 all powerful and flexible message logging mechanism
ii liblog-message-simple-perl 0.10-2 all simplified interface to Log::Message
ii liblogging-stdlog0 1.0.4-1 amd64 easy to use and lightweight logging library
ii liblognorm1 1.0.1-3 amd64 Log normalizing library
ii liblsan0 4.9.2-10+deb8u2 amd64 LeakSanitizer -- a memory leak detector (runtime)
rc liblua5.1-0 5.1.5-7.1 amd64 Shared library for the Lua interpreter version 5.1
ii liblwp-mediatypes-perl 6.02-1 all module to guess media type for a file or a URL
ii liblwp-protocol-https-perl 6.06-2 all HTTPS driver for LWP::UserAgent
ii liblwres90 1:9.9.5.dfsg-9+deb8u17 amd64 Lightweight Resolver Library used by BIND
ii liblzma5 5.1.1alpha+20120614-2+b3 amd64 XZ-format compression library
ii libmagic1 1:5.22+15-2+deb8u5 amd64 File type determination library using "magic" numbers
ii libmailtools-perl 2.13-1 all Manipulate email in perl programs
ii libmnl0 1.0.3-5 amd64 minimalistic Netlink communication library
ii libmodule-build-perl 0.421000-2+deb8u1 all framework for building and installing Perl modules
ii libmodule-pluggable-perl 5.1-1 all module for giving modules the ability to have plugins
ii libmodule-signature-perl 0.73-1+deb8u2 all module to manipulate CPAN SIGNATURE files
ii libmount1 2.25.2-6 amd64 device mounting library
ii libmpc3 1.0.2-1 amd64 multiple precision complex floating-point library
ii libmpfr4 3.1.2-2 amd64 multiple precision floating-point computation
ii libmro-compat-perl 0.12-1 all mro::* interface compatibility for Perls < 5.9.5
ii libmysqlclient18 5.5.62-0+deb8u1 amd64 MySQL database client library
ii libncurses5 5.9+20140913-1+deb8u2 amd64 shared libraries for terminal handling
ii libncurses5-dev 5.9+20140913-1+deb8u2 amd64 developer's libraries for ncurses
ii libncursesw5 5.9+20140913-1+deb8u2 amd64 shared libraries for terminal handling (wide character support)
ii libnet-http-perl 6.07-1 all module providing low-level HTTP connection client
ii libnet-smtp-ssl-perl 1.01-3 all Perl module providing SSL support to Net::SMTP
ii libnet-ssleay-perl 1.65-1+deb8u1 amd64 Perl module for Secure Sockets Layer (SSL)
ii libnetfilter-acct1 1.0.2-1.1 amd64 Netfilter acct library
ii libnettle4 2.7.1-5+deb8u2 amd64 low level cryptographic library (symmetric and one-way cryptos)
ii libnewt0.52 0.52.17-1+b1 amd64 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.1-3 amd64 Netfilter netlink library
ii libnfsidmap2 0.25-5 amd64 NFS idmapping library
ii libonig2 5.9.5-3.2+deb8u1 amd64 Oniguruma regular expressions library
ii libp11-kit0 0.20.7-1 amd64 Library for loading and coordinating access to PKCS#11 modules - runtime
ii libpackage-constants-perl 0.04-1 all List constants defined in a package
ii libpam-modules 1.1.8-3.1+deb8u2+b1 amd64 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.1.8-3.1+deb8u2+b1 amd64 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.8-3.1+deb8u2 all Runtime support for the PAM library
ii libpam0g 1.1.8-3.1+deb8u2+b1 amd64 Pluggable Authentication Modules library
ii libpango-1.0-0 1.36.8-3 amd64 Layout and rendering of internationalized text
ii libpangocairo-1.0-0 1.36.8-3 amd64 Layout and rendering of internationalized text
ii libpangoft2-1.0-0 1.36.8-3 amd64 Layout and rendering of internationalized text
ii libpaper-utils 1.1.24+nmu4 amd64 library for handling paper characteristics (utilities)
ii libpaper1 1.1.24+nmu4 amd64 library for handling paper characteristics
ii libparams-util-perl 1.07-2+b1 amd64 Perl extension for simple stand-alone param checking functions
ii libparse-debianchangelog-perl 1.2.0-1.1 all parse Debian changelogs and output them in other formats
ii libpci3 1:3.2.1-3 amd64 Linux PCI Utilities (shared library)
ii libpcre3 2:8.35-3.3+deb8u4 amd64 Perl 5 Compatible Regular Expression Library - runtime files
ii libperl4-corelibs-perl 0.003-1 all libraries historically supplied with Perl 4
ii libpipeline1 1.4.0-1 amd64 pipeline manipulation library
ii libpixman-1-0 0.32.6-3+deb8u1 amd64 pixel-manipulation library for X and cairo
ii libpng12-0 1.2.50-2+deb8u3 amd64 PNG library - runtime
ii libpod-latex-perl 0.61-1 all module to convert Pod data to formatted LaTeX
ii libpod-readme-perl 0.11-1 all Perl module to convert POD to README file
ii libpopt0 1.16-10 amd64 lib for parsing cmdline parameters
ii libprocps3 2:3.3.9-9+deb8u1 amd64 library for accessing process information from /proc
ii libpsl0 0.5.1-1 amd64 Library for Public Suffix List (shared libraries)
ii libpth20 2.0.7-20 amd64 GNU Portable Threads
ii libpython-stdlib 2.7.9-1 amd64 interactive high-level object-oriented language (default python version)
ii libpython2.7-minimal 2.7.9-2+deb8u2 amd64 Minimal subset of the Python language (version 2.7)
ii libpython2.7-stdlib 2.7.9-2+deb8u2 amd64 Interactive high-level object-oriented language (standard library, version 2.7)
ii libqdbm14 1.8.78-5+b1 amd64 QDBM Database Libraries without GDBM wrapper[runtime]
ii libquadmath0 4.9.2-10+deb8u2 amd64 GCC Quad-Precision Math Library
ii libreadline6 6.3-8+b3 amd64 GNU readline and history libraries, run-time libraries
ii libregexp-common-perl 2013031301-1 all module with common regular expressions
```

```
ii librtmp1 2.4+20150115.gita107cef-1+deb8u1 amd64 toolkit for RTMP streams (shared library)
ii libsasl2-2 2.1.26.dfsg1-13+deb8u1 amd64 Cyrus SASL - authentication abstraction library
ii libsasl2-modules 2.1.26.dfsg1-13+deb8u1 amd64 Cyrus SASL - pluggable authentication modules
ii libsasl2-modules-db 2.1.26.dfsg1-13+deb8u1 amd64 Cyrus SASL - pluggable authentication modules (DB)
ii libselinux1 2.3-2 amd64 SELinux runtime shared libraries
ii libsemanage-common 2.3-1 all Common files for SELinux policy management libraries
ii libsemanage1 2.3-1+b1 amd64 SELinux policy management library
ii libsepol1 2.3-2 amd64 SELinux library for manipulating binary security policies
ii libsigc++-2.0-0c2a 2.4.0-1 amd64 type-safe Signal Framework for C++ - runtime
ii libsigsegv2 2.10-4+b1 amd64 Library for handling page faults in a portable way
ii libslang2 2.3.0-2 amd64 S-Lang programming library - runtime version
ii libsmartcols1 2.25.2-6 amd64 smart column output alignment library
ii libsoftware-license-perl 0.103010-3 all module providing templated software licenses
ii libsqlite3-0 3.8.7.1-1+deb8u4 amd64 SQLite 3 shared library
ii libss2 1.42.12-2+b1 amd64 command-line interface parsing library
ii libssh2-1 1.4.3-4.1+deb8u3 amd64 SSH2 client-side library
ii libssl1.0.0 1.0.1t-1+deb8u11 amd64 Secure Sockets Layer toolkit - shared libraries
ii libstdc++-4.9-dev 4.9.2-10+deb8u2 amd64 GNU Standard C++ Library v3 (development files)
ii libstdc++6 4.9.2-10+deb8u2 amd64 GNU Standard C++ Library v3
ii libsub-exporter-perl 0.986-1 all sophisticated exporter for custom-built routines
ii libsub-install-perl 0.928-1 all module for installing subroutines into packages easily
ii libsub-name-perl 0.12-1 amd64 module for assigning a new name to referenced sub
ii libswitch-perl 2.17-2 all switch statement for Perl
ii libsystemd0 215-17+deb8u11 amd64 systemd utility library
ii libtasn1-6 4.2-3+deb8u3 amd64 Manage ASN.1 structures (runtime)
ii libterm-readkey-perl 2.32-1+b1 amd64 perl module for simple terminal control
ii libterm-ui-perl 0.42-1 all Term::ReadLine UI made easy
ii libtext-charwidth-perl 0.04-7+b3 amd64 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5+b2 amd64 converts between character sets in Perl
ii libtext-soundex-perl 3.4-1+b2 amd64 implementation of the soundex algorithm
ii libtext-template-perl 1.46-1 all perl module to process text templates
ii libtext-unidecode-perl 1.22-1 all Text::Unidecode -- US-ASCII transliterations of Unicode text
ii libtext-wrapi18n-perl 0.06-7 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.21-1 all Data files for Thai language support library
ii libthai0 0.1.21-1 amd64 Thai language support library
ii libtiff5 4.0.3-12.3+deb8u8 amd64 Tag Image File Format (TIFF) library
ii libtimedate-perl 2.3000-2 all collection of modules to manipulate date/time information
ii libtinfo-dev 5.9+20140913-1+deb8u2 amd64 developer's library for the low-level terminfo library
ii libtinfo5 5.9+20140913-1+deb8u2 amd64 shared low-level terminfo library for terminal handling
ii libtirpc1 0.2.5-1+deb8u2 amd64 transport-independent RPC library
ii libtokyocabinet9 1.4.48-3 amd64 Tokyo Cabinet Database Libraries [runtime]
ii libtsan0 4.9.2-10+deb8u2 amd64 ThreadSanitizer -- a Valgrind-based detector of data races (runtime)
ii libubsan0 4.9.2-10+deb8u2 amd64 UBSan -- undefined behaviour sanitizer (runtime)
ii libudev1 215-17+deb8u11 amd64 libudev shared library
ii liburi-perl 1.64-1 all module to manipulate and access URI strings
ii libusb-0.1-4 2:0.1.12-25 amd64 userspace USB programming library
ii libusb-1.0-0 2:1.0.19-1 amd64 userspace USB programming library
ii libustr-1.0-1 1.0.4-3+b2 amd64 Micro string library: shared library
ii libuuid1 2.25.2-6 amd64 Universally Unique ID library
ii libvpx1 1.3.0-3+deb8u1 amd64 VP8 and VP9 video codec (shared library)
ii libwebp5 0.4.1-1.2+b2 amd64 Lossy compression of digital photographic images.
ii libwebpdemux1 0.4.1-1.2+b2 amd64 Lossy compression of digital photographic images.
ii libwebpmux1 0.4.1-1.2+b2 amd64 Lossy compression of digital photographic images.
ii libwrap0 7.6.q-25 amd64 Wietse Venema's TCP wrappers library
ii libwww-perl 6.08-1 all simple and consistent interface to the world-wide web
ii libwww-robotrules-perl 6.01-1 all database of robots.txt-derived permissions
ii libx11-6 2:1.6.2-3+deb8u2 amd64 X11 client-side library
ii libx11-data 2:1.6.2-3+deb8u2 all X11 client-side library
ii libxapian22 1.2.19-1+deb8u1 amd64 Search engine library
ii libxau6 1:1.0.8-1 amd64 X11 authorisation library
ii libxcb-render0 1.10-3+b1 amd64 X C Binding, render extension
ii libxcb-shm0 1.10-3+b1 amd64 X C Binding, shm extension
ii libxcb1 1.10-3+b1 amd64 X C Binding
ii libxcomposite1 1:0.4.4-1 amd64 X11 Composite extension library
ii libxcursor1 1:1.1.14-1+deb8u2 amd64 X cursor management library
ii libxdamage1 1:1.1.4-2+b1 amd64 X11 damaged region extension library
ii libxdmcp6 1:1.1.1-1+b1 amd64 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.3-1 amd64 X11 miscellaneous extension library
ii libxfixes3 1:5.0.1-2+deb8u1 amd64 X11 miscellaneous 'fixes' extension library
ii libxi6 2:1.7.4-1+deb8u1 amd64 X11 Input extension library
ii libxinerama1 2:1.1.3-1+b1 amd64 X11 Xinerama extension library
ii libxml-libxml-perl 2.0116+dfsg-1+deb8u2 amd64 Perl interface to the libxml2 library
ii libxml-namespacesupport-perl 1.11-1 all Perl module for supporting simple generic namespaces
ii libxml-parser-perl 2.41-3 amd64 Perl module for parsing XML files
ii libxml-sax-base-perl 1.07-1 all base class for SAX drivers and filters
ii libxml-sax-expat-perl 0.40-2 all Perl module for a SAX2 driver for Expat (XML::Parser)
ii libxml-sax-perl 0.99+dfsg-2 all Perl module for using and building Perl SAX2 XML processors
ii libxml2 2.9.1+dfsg1-5+deb8u7 amd64 GNOME XML library
ii libxmuu1 2:1.1.2-1 amd64 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.12-0+deb8u1 amd64 X11 pixmap library
ii libxrandr2 2:1.4.2-1+deb8u1 amd64 X11 RandR extension library
ii libxrender1 1:0.9.8-1+b1 amd64 X Rendering Extension client library
ii libxslt1.1 1.1.28-2+deb8u4 amd64 XSLT 1.0 processing library - runtime library
ii libxtables10 1.4.21-2+b1 amd64 netfilter xtables library
ii linux-base 4.5~deb8u1 all Linux image base package
ii linux-image-3.16.0-4-amd64 3.16.51-2 amd64 Linux 3.16 for 64-bit PCs
ii linux-image-amd64 3.16+63 amd64 Linux for 64-bit PCs (meta-package)
ii linux-libc-dev 3.16.64-2 amd64 Linux support headers for userspace development
ii locales 2.19-18+deb8u10 all GNU C Library: National Language (locale) data [support]
ii login 1:4.2-3+deb8u4 amd64 system login tools
ii logrotate 3.8.7-1+b1 amd64 Log rotation utility
ii lsb-base 4.1+Debian13+nmu1 all Linux Standard Base 4.1 init script functionality
ii lsb-release 4.1+Debian13+nmu1 all Linux Standard Base version reporting utility
ii lsof 4.86+dfsg-1 amd64 Utility to list open files
ii m4 1.4.17-4 amd64 macro processing language
ii make 4.0-8.1 amd64 utility for directing compilation
ii man-db 2.7.0.2-5 amd64 on-line manual pager
ii manpages 3.74-1 all Manual pages about using a GNU/Linux system
ii manpages-dev 3.74-1 all Manual pages about using GNU/Linux for development
```

```
ii mawk 1.3.3-17 amd64 a pattern scanning and text processing language
ii mime-support 3.58 all MIME files 'mime.types' & 'mailcap', and support programs
ii mlocate 0.26-1 amd64 quickly find files on the filesystem based on their name
ii mount 2.25.2-6 amd64 Tools for mounting and manipulating filesystems
ii multiarch-support 2.19-18+deb8u10 amd64 Transitional package to ensure multiarch compatibility
ii mutt 1.5.23-3+deb8u1 amd64 text-based mailreader supporting MIME, GPG, PGP and threading
ii mysql-client-5.5 5.5.62-0+deb8u1 amd64 MySQL database client binaries
ii mysql-common 5.5.62-0+deb8u1 all MySQL database common files, e.g. /etc/mysql/my.cnf
ii mysql-server 5.5.62-0+deb8u1 all MySQL database server (metapackage depending on the latest version)
ii mysql-server-5.5 5.5.62-0+deb8u1 amd64 MySQL database server binaries and system database setup
ii mysql-server-core-5.5 5.5.62-0+deb8u1 amd64 MySQL database server binaries
ii nano 2.2.6-3 amd64 small, friendly text editor inspired by Pico
ii ncurses-base 5.9+20140913-1+deb8u2 all basic terminal type definitions
ii ncurses-bin 5.9+20140913-1+deb8u2 amd64 terminal-related programs and man pages
ii ncurses-term 5.9+20140913-1+deb8u2 all additional terminal type definitions
ii net-tools 1.60-26+b1 amd64 NET-3 networking toolkit
ii netbase 5.3 all Basic TCP/IP networking system
ii netcat-traditional 1.10-41 amd64 TCP/IP swiss army knife
ii nfacct 1.0.1-1.1 amd64 netfilter accounting object tool
ii nfs-common 1:1.2.8-9 amd64 NFS support files common to client and server
ii nginx 1.6.2-5+deb8u6 all small, powerful, scalable web/proxy server
ii nginx-common 1.6.2-5+deb8u6 all small, powerful, scalable web/proxy server - common files
ii nginx-full 1.6.2-5+deb8u6 amd64 nginx web/proxy server (standard version)
ii openssh-client 1:6.7p1-5+deb8u8 amd64 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:6.7p1-5+deb8u8 amd64 secure shell (SSH) server, for secure access from remote machines
ii openssh-sftp-server 1:6.7p1-5+deb8u8 amd64 secure shell (SSH) sftp server module, for SFTP access from remote machines
ii openssl 1.0.1t-1+deb8u11 amd64 Secure Sockets Layer toolkit - cryptographic utility
ii os-prober 1.65+deb8u1 amd64 utility to detect other OSes on a set of drives
ii passwd 1:4.2-3+deb8u4 amd64 change and administer password and group data
ii patch 2.7.5-1 amd64 Apply a diff file to an original
ii pciutils 1:3.2.1-3 amd64 Linux PCI Utilities
ii perl 5.20.2-3+deb8u12 amd64 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.20.2-3+deb8u12 amd64 minimal Perl system
ii perl-modules 5.20.2-3+deb8u12 all Core Perl modules
ii php5 5.6.40+dfsg-0+deb8u2 all server-side, HTML-embedded scripting language (metapackage)
ii php5-cgi 5.6.40+dfsg-0+deb8u2 amd64 server-side, HTML-embedded scripting language (CGI binary)
ii php5-cli 5.6.40+dfsg-0+deb8u2 amd64 command-line interpreter for the php5 scripting language
ii php5-common 5.6.40+dfsg-0+deb8u2 amd64 Common files for packages built from the php5 source
ii php5-fpm 5.6.40+dfsg-0+deb8u2 amd64 server-side, HTML-embedded scripting language (FPM-CGI binary)
ii php5-json 1.3.6-1 amd64 JSON module for php5
ii php5-readline 5.6.40+dfsg-0+deb8u2 amd64 Readline module for php5
ii pinentry-gtk2 0.8.3-2 amd64 GTK+-2-based PIN or pass-phrase entry dialog for GnuPG
ii procmail 3.22-24+deb8u1 amd64 Versatile e-mail processor
ii procps 2:3.3.9-9+deb8u1 amd64 /proc file system utilities
ii psmisc 22.21-2 amd64 utilities that use the proc file system
ii python 2.7.9-1 amd64 interactive high-level object-oriented language (default version)
ii python-apt 0.9.3.12 amd64 Python interface to libapt-pkg
ii python-apt-common 0.9.3.12 all Python interface to libapt-pkg (locales)
ii python-cffi 0.8.6-1 amd64 Foreign Function Interface for Python calling C code
ii python-chardet 2.3.0-1 all universal character encoding detector for Python2
ii python-cryptography 0.6.1-1+deb8u1 amd64 Python library exposing cryptographic recipes and primitives (Python 2)
ii python-debian 0.1.27 all Python modules to work with Debian-related data formats
ii python-debianbts 1.12 all Python interface to Debian's Bug Tracking System
ii python-defusedxml 0.4.1-2 all XML bomb protection for Python stdlib modules (for Python 2)
ii python-docutils 0.12+dfsg-1 all text processing system for reStructuredText (implemented in Python 2)
ii python-minimal 2.7.9-1 amd64 minimal subset of the Python language (default version)
ii python-ndg-httpsclient 0.3.2-1 all enhanced HTTPS support for httplib and urllib2 using PyOpenSSL
ii python-openssl 0.14-1 all Python 2 wrapper around the OpenSSL library
ii python-pil 2.6.1-2+deb8u3 amd64 Python Imaging Library (Pillow fork)
ii python-pkg-resources 5.5.1-1 all Package Discovery and Resource Access using pkg_resources
ii python-ply 3.4-5 all Lex and Yacc implementation for Python2
ii python-pyasn1 0.1.7-1 all ASN.1 library for Python (Python 2 module)
ii python-pycparser 2.10+dfsg-3 all C parser in Python
ii python-pygments 2.0.1+dfsg-1.1+deb8u1 all syntax highlighting package written in Python
ii python-reportbug 6.6.3+deb8u2 all Python modules for interacting with bug tracking systems
ii python-requests 2.4.3-6 all elegant and simple HTTP library for Python2, built for human beings
ii python-roman 2.0.0-1 all module for generating/analyzing Roman numerals for Python 2
ii python-six 1.8.0-1 all Python 2 and 3 compatibility library (Python 2 interface)
ii python-soappy 0.12.22-1 all SOAP Support for Python
ii python-support 1.0.15 all automated rebuilding support for Python modules
ii python-urllib3 1.9.1-3 all HTTP library with thread-safe connection pooling for Python
ii python-wstools 0.4.3-2 all WSDL parsing tools Python module
ii python2.7 2.7.9-2+deb8u2 amd64 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.9-2+deb8u2 amd64 Minimal subset of the Python language (version 2.7)
ii readline-common 6.3-8 all GNU readline and history libraries, common files
ii rename 0.20-3 all Perl extension for renaming multiple files
ii reportbug 6.6.3+deb8u2 all reports bugs in the Debian distribution
ii rpcbind 0.2.1-6+deb8u2 amd64 converts RPC program numbers into universal addresses
ii rsyslog 8.4.2-1+deb8u2 amd64 reliable system and kernel logging daemon
ii sed 4.2.2-4+deb8u1 amd64 The GNU sed stream editor
ii sensible-utils 0.0.9+deb8u1 all Utilities for sensible alternative selection
ii sgml-base 1.26+nmu4 all SGML infrastructure and SGML catalog file support
ii shared-mime-info 1.3-1 amd64 FreeDesktop.org shared MIME database and spec
ii ssl-cert 1.0.35 all simple debconf wrapper for OpenSSL
ii startpar 0.59-3 amd64 run processes in parallel and multiplex their output
ii systemd 215-17+deb8u11 amd64 system and service manager
ii systemd-sysv 215-17+deb8u11 amd64 system and service manager - SysV links
ii sysv-rc 2.88dsf-59 all System-V-like runlevel change mechanism
ii sysvinit-utils 2.88dsf-59 amd64 System-V-like utilities
ii tar 1.27.1-2+deb8u2 amd64 GNU version of the tar archiving utility
ii task-english 3.31+deb8u1 all General English environment
ii tasksel 3.31+deb8u1 all tool for selecting tasks for installation on Debian systems
ii tasksel-data 3.31+deb8u1 all official tasks used for installation of Debian systems
ii tcpd 7.6.q-25 amd64 Wietse Venema's TCP wrapper utilities
ii telnet 0.17-36 amd64 The telnet client
ii texinfo 5.2.0.dfsg.1-6 amd64 Documentation system for on-line information and printed output
ii time 1.7-25 amd64 GNU time program for measuring CPU resource usage
ii traceroute 1:2.0.20-2+b1 amd64 Traces the route taken by packets over an IPv4/IPv6 network
ii tzdata 2019a-0+deb8u1 all time zone and daylight-saving time data
```

```
ii ucf 3.0030 all Update Configuration File(s): preserve user changes to config files
ii udev 215-17+deb8u11 amd64 /dev/ and hotplug management daemon
ii usbutils 1:007-2 amd64 Linux USB utilities
ii util-linux 2.25.2-6 amd64 Miscellaneous system utilities
ii util-linux-locales 2.25.2-6 all Locales files for util-linux
ii vim-common 2:7.4.488-7+deb8u3 amd64 Vi IMproved - Common files
ii vim-tiny 2:7.4.488-7+deb8u3 amd64 Vi IMproved - enhanced vi editor - compact version
ii w3m 0.5.3-19+deb8u2 amd64 WWW browsable pager with excellent tables/frames support
ii wamerican 7.1-1 all American English dictionary words for /usr/share/dict
ii wget 1.16-1+deb8u5 amd64 retrieves files from the web
ii whiptail 0.52.17-1+b1 amd64 Displays user-friendly dialog boxes from shell scripts
ii whois 5.2.7 amd64 intelligent WHOIS client
ii xauth 1:1.0.9-1 amd64 X authentication utility
ii xdg-user-dirs 0.15-2 amd64 tool to manage well known user directories
ii xkb-data 2.12-1 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.13+nmu2 all XML infrastructure and XML catalog file support
ii xz-utils 5.1.1alpha+20120614-2+b3 amd64 XZ-format compression utilities
ii zlib1g 1:1.2.8.dfsg-2+b1 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: 'yash'
Port: 22
Proto: SSH
Method: password


See the output of the following plugin for details :

Plugin ID : 102094
Plugin Name : SSH Commands Require Privilege Escalation
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided -

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User: 'yash'
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 3.16.0-4-amd64 Sun Nov 9 01:50 - 04:46 (02:55)
reboot system boot 3.16.0-4-amd64 Sat Apr 20 21:04 - 21:17 (00:12)
reboot system boot 3.16.0-4-amd64 Sat Apr 20 20:13 - 20:38 (00:24)
reboot system boot 3.16.0-4-amd64 Fri Apr 19 23:33 - 23:49 (00:16)

wtmp begins Fri Apr 19 23:33:21 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 10.50.41.33 to 10.50.41.35 :
10.50.41.33
10.50.41.35

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 : /lib/x86_64-linux-gnu/liblzma.so.5.0.0
Version : 5.1.1
Associated Package : liblzma5 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package

Path : /usr/bin/xz
Version : 5.1.1
Associated Package : xz-utils 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package
```

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 0.5 111140 5308 ? Ss 01:50 0:01 /sbin/init
root 2 0.0 0.0 0 0 ? S 01:50 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 01:50 0:05 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< 01:50 0:00 [kworker/0:0H]
root 6 0.0 0.0 0 0 ? S 01:50 0:01 [kworker/u2:0]
root 7 0.0 0.0 0 0 ? S 01:50 0:01 [rcu_sched]
root 8 0.0 0.0 0 0 ? S 01:50 0:00 [rcu_bh]
root 9 0.0 0.0 0 0 ? S 01:50 0:00 [migration/0]
root 10 0.0 0.0 0 0 ? S 01:50 0:00 [watchdog/0]
root 11 0.0 0.0 0 0 ? S< 01:50 0:00 [khelper]
root 12 0.0 0.0 0 0 ? S 01:50 0:00 [kdevtmpfs]
root 13 0.0 0.0 0 0 ? S< 01:50 0:00 [netns]
root 14 0.0 0.0 0 0 ? S 01:50 0:00 [khungtaskd]
root 15 0.0 0.0 0 0 ? S< 01:50 0:00 [writeback]
root 16 0.0 0.0 0 0 ? SN 01:50 0:00 [ksmd]
root 17 0.0 0.0 0 0 ? SN 01:50 0:00 [khugepaged]
root 18 0.0 0.0 0 0 ? S< 01:50 0:00 [crypto]
root 19 0.0 0.0 0 0 ? S< 01:50 0:00 [kintegrityd]
root 20 0.0 0.0 0 0 ? S< 01:50 0:00 [bioset]
root 21 0.0 0.0 0 0 ? S< 01:50 0:00 [kblockd]
root 23 0.0 0.0 0 0 ? S 01:50 0:00 [kswapd0]
root 24 0.0 0.0 0 0 ? S< 01:50 0:00 [vmstat]
root 25 0.0 0.0 0 0 ? S 01:50 0:00 [fsnotify_mark]
root 31 0.0 0.0 0 0 ? S< 01:50 0:00 [kthrotld]
root 32 0.0 0.0 0 0 ? S< 01:50 0:00 [ipv6_addrconf]
root 33 0.0 0.0 0 0 ? S< 01:50 0:00 [deferwq]
root 67 0.0 0.0 0 0 ? S< 01:50 0:00 [kpsmoused]
```

```
root 70 0.0 0.0 0 0 ? S 01:50 0:00 [khubd]
root 72 0.0 0.0 0 0 ? S< 01:50 0:00 [ata_sff]
root 73 0.0 0.0 0 0 ? S 01:50 0:00 [scsi_eh_0]
root 74 0.0 0.0 0 0 ? S< 01:50 0:00 [scsi_tmf_0]
root 75 0.0 0.0 0 0 ? S 01:50 0:00 [kworker/u2:2]
root 76 0.0 0.0 0 0 ? S 01:50 0:00 [scsi_eh_1]
root 77 0.0 0.0 0 0 ? S< 01:50 0:00 [scsi_tmf_1]
root 78 0.0 0.0 0 0 ? S 01:50 0:00 [scsi_eh_2]
root 79 0.0 0.0 0 0 ? S< 01:50 0:00 [scsi_tmf_2]
root 84 0.0 0.0 0 0 ? S< 01:50 0:01 [kworker/0:1H]
root 105 0.0 0.0 0 0 ? S 01:50 0:00 [jbd2/sda1-8]
root 106 0.0 0.0 0 0 ? S< 01:50 0:00 [ext4-rsv-conver]
root 136 0.0 0.0 0 0 ? S 01:50 0:00 [kauditd]
root 139 0.0 0.3 28872 3596 ? Ss 01:50 0:00 /lib/systemd/systemd-journald
root 146 0.0 0.3 40816 3228 ? Ss 01:50 0:00 /lib/systemd/systemd-udevd
root 379 0.0 0.8 25400 8792 ? Ss 01:50 0:01 dhclient -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases eth0
root 400 0.0 0.2 37164 2888 ? Ss 01:50 0:00 /sbin/rpcbind -w
statd 409 0.0 0.2 37332 3016 ? Ss 01:50 0:00 /sbin/rpc.statd
root 414 0.0 0.0 0 0 ? S< 01:50 0:00 [rpciod]
root 416 0.0 0.0 0 0 ? S< 01:50 0:00 [nfsiod]
root 423 0.0 0.0 23356 204 ? Ss 01:50 0:00 /usr/sbin/rpc.idmapd
daemon 425 0.0 0.1 19024 1868 ? Ss 01:50 0:00 /usr/sbin/atd -f
root 426 0.0 0.2 27504 2908 ? Ss 01:50 0:00 /usr/sbin/cron -f
root 429 0.0 0.2 19856 2596 ? Ss 01:50 0:00 /lib/systemd/systemd-logind
message+ 432 0.0 0.3 42124 3380 ? Ss 01:50 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-
activation
root 447 0.0 0.3 258672 3608 ? Ssl 01:50 0:00 /usr/sbin/rsyslogd -n
root 448 0.0 0.1 4256 1672 ? Ss 01:50 0:00 /usr/sbin/acpid
root 456 0.0 0.2 63316 2988 tty1 Ss 01:50 0:00 /bin/login --
root 465 0.0 0.2 91200 2972 ? Ss 01:50 0:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
www-data 466 0.0 0.4 91848 5012 ? S 01:50 0:09 nginx: worker process
www-data 467 0.0 0.4 91848 4748 ? S 01:50 0:09 nginx: worker process
www-data 468 0.0 0.4 91848 5016 ? S 01:50 0:08 nginx: worker process
www-data 469 0.1 0.4 91884 4912 ? S 01:50 0:13 nginx: worker process
root 476 0.0 1.9 174588 20316 ? Ss 01:50 0:02 php-fpm: master process (/etc/php5/fpm/php-fpm.conf)
www-data 485 0.0 1.6 176696 17368 ? S 01:50 0:00 php-fpm: pool www
root 488 0.0 0.1 4336 1620 ? S 01:50 0:00 /bin/sh /usr/bin/mysqld_safe
mysql 832 0.1 4.5 558176 46668 ? Sl 01:50 0:19 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib/mysql/plugin --user=mysql --log-error=/var/log/mysql/error.log --pid-file=/var/run/mysqld/mysqld.pid --
socket=/var/run/mysqld/mysqld.sock --port=3306
Debian-+ 1226 0.0 0.3 53284 3368 ? Ss 01:50 0:00 /usr/sbin/exim4 -bd -q30m
www-data 1376 0.0 1.7 176696 17604 ? S 02:59 0:00 php-fpm: pool www
root 17312 0.0 0.5 55180 5480 ? Ss 04:24 0:00 /usr/sbin/sshd -D
root 17411 0.1 0.0 0 0 ? S 04:27 0:01 [kworker/0:1]
yash 17436 0.0 0.0 4336 800 tty1 S+ 04:30 0:00 -sh
www-data 17441 0.0 0.8 174588 9088 ? S 04:37 0:00 php-fpm: pool www
root 17442 0.0 0.0 0 0 ? S 04:37 0:00 [kworker/0:2]
root 17496 0.1 0.0 0 0 ? S 04:42 0:00 [kworker/0:0]
root 17963 0.1 0.5 80160 5916 ? Ss 04:46 0:00 sshd: yash [priv]
root 17977 0.0 0.5 57252 5532 ? Ss 04:46 0:00 sshd: [accepted]
sshd 17978 0.0 0.3 55180 3144 ? S 04:46 0:00 sshd: [net]
yash 17979 0.0 0.4 80324 4716 ? S 04:46 0:00 sshd: yash@notty
yash 17980 0.0 0.0 4336 768 ? Ss 04:46 0:00 sh -c /bin/ps auxww 2>/dev/null
yash 17981 0.0 0.2 19104 2456 ? R 04:46 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:

unzip -v :
Could not chdir to home directory /home/yash: No such file or directorysh: 1: unzip: not found


Account : yash
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 : 7.4
```

182848 - libcurl Installed (Linux / Unix) -

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.3.0
Version : 7.38.0
Associated Package : libcurl3-gnutls 7.38.0-4
Managed by OS : True
```

106375 - nginx HTTP Server Detection -

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

https://nginx.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL : http://10.50.41.35/
Version : 1.6.2
source : Server: nginx/1.6.2
```

136340 - nginx Installed (Linux/UNIX) -

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

https://www.nginx.com

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of nginx:

Path : nginx (via package manager)
Version : 1.6.2-5

Path : /usr/sbin/nginx
Version : 1.6.2
Associated Package : nginx-full: /usr/sbin/nginx
Detection Method : Running Process
Full Version : 1.6.2
Managed by OS : True
Nginx Plus : False
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 98% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Debian DLA-2241-2 : linux security update: Upgrade the affected packages.	173	1
Debian DSA-4196-1 : linux - security update: Upgrade the linux packages. For the oldstable distribution (jessie), these problems have been fixed in version 3.16.56-1+deb8u1. This update includes various fixes for regressions from 3.16.56-1 as released in DSA-4187-1 (Cf. #897427, #898067 and #898100). For the stable distribution (stretch), these problems have been fixed in version 4.9.88-1+deb9u1. The fix for CVE-2018-1108 applied in DSA-4188-1 is temporarily reverted due to various regression, cf. #897599.	50	1
Debian DLA-2261-1 : php5 security update: Upgrade the affected packages.	20	1
Debian DLA-1925-1 : python2.7 security update: Upgrade the affected packages.	9	1
Debian DLA-2009-1 : tiff security update: Upgrade the affected packages.	6	1
Debian DLA-2237-1 : cups security update: Upgrade the affected packages.	6	1
Debian DLA-1973-1 : libxslt security update: Upgrade the affected packages.	5	1

Debian DLA-2020-1 : libonig security update: Upgrade the affected libonig-dev, libonig2, and libonig2-dbg packages.	5	1
Debian DLA-1909-1 : freetype security update: Upgrade the affected packages.	4	1
Debian DLA-2085-1 : zlib security update: Upgrade the affected packages.	4	1
Debian DLA-1871-1 : vim security update: Upgrade the affected packages.	3	1
Debian DLA-2136-1 : libvpx security update: Upgrade the affected packages.	3	1
Debian DLA-2199-1 : openldap security update: Upgrade the affected packages.	3	1
Debian DLA-2227-1 : bind9 security update: Upgrade the affected packages.	3	1
Debian DLA-1864-1 : patch security update: Upgrade the affected patch package.	2	1
Debian DLA-1866-2 : glib2.0 regression update: Upgrade the affected packages.	2	1
Debian DLA-1917-1 : curl security update: Upgrade the affected packages.	2	1
Debian DLA-1932-1 : openssl security update: Upgrade the affected packages.	2	1
Debian DLA-1991-1 : libssh2 security update: Upgrade the affected packages.	2	1
Debian DLA-2074-1 : python-apt security update: Upgrade the affected packages.	2	1
Debian DLA-2106-1 : libgd2 security update: Upgrade the affected packages.	2	1
Debian DLA-2156-1 : e2fsprogs security update: Upgrade the affected packages.	2	1
Debian DLA-2195-1 : w3m security update: Upgrade the affected w3m, and w3m-img packages.	2	1
Debian DLA-2213-1 : exim4 security update: Upgrade the affected packages.	2	1
Debian DLA-2221-1 : sqlite3: Upgrade the affected packages.	2	1
Debian DLA-2235-1 : dbus security update: Upgrade the affected packages.	2	1
Debian DLA-2268-2 : mutt regression update: Upgrade the affected mutt, mutt-dbg, and mutt-patched packages.	2	1
Debian DLA-1828-1 : python-urllib3 security update: Upgrade the affected packages.	1	1
Debian DLA-1839-1 : expat security update: Upgrade the affected packages.	1	1
Debian DLA-1931-2 : libgcrypt20 regression update: Upgrade the affected packages.	1	1
Debian DLA-1969-1 : file security update: Upgrade the affected packages.	1	1
Debian DLA-1981-1 : cpio security update: Upgrade the affected cpio, and cpio-win32 packages.	1	1
Debian DLA-2003-1 : isc-dhcp security update: Upgrade the affected packages.	1	1
Debian DLA-2006-1 : libxdmcp security update: Upgrade the affected packages.	1	1
Debian DLA-2040-1 : harfbuzz security update: Upgrade the affected packages.	1	1
Debian DLA-2044-1 : cyrus-sasl2 security update: Upgrade the affected packages.	1	1
Debian DLA-2048-1 : libxml2 security update: Upgrade the affected packages.	1	1
Debian DLA-2052-1 : libbsd security update: Upgrade the affected libbsd-dev, libbsd0, and libbsd0-dbg packages.	1	1
Debian DLA-2086-1 : wget security update: Upgrade the affected wget package.	1	1
Debian DLA-2151-1 : icu security update: Upgrade the affected packages.	1	1
Debian DLA-2210-1 : apt security update: Upgrade the affected packages.	1	1
Debian DLA-2228-2 : json-c regression update: Upgrade the affected packages.	1	1
Debian DLA-2255-1 : libtasn1-6 security update: Upgrade the affected packages.	1	1

Debian DLA-2256-1 : libtirpc security update: Upgrade the affected libtirpc-dev, and libtirpc1 packages.	1	1
MySQL Denial of Service (Jul 2020 CPU): Refer to the vendor advisory.	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
nginx < 1.17.7 Information Disclosure: Upgrade to nginx version 1.17.7 or later.	1	1