tenable Nessus

Report generated by Tenable Nessus™

SickOS 1.1

Thu, 13 Nov 2025 17:32:20 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.136.108.108

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	18	19	4	63

Scan Information

Start time:	Thu Nov 13 17:23:12 2025
End time:	Thu Nov 13 17:32:19 2025

Host Information

IP:	10.136.108.108
MAC Address:	08:00:27:C6:38:3F
OS:	Linux Kernel 3.11.0-15-generic on Ubuntu 12.04

Vulnerabilities

77823 - Bash Remote Code Execution (Shellshock) -

Synopsis

A system shell on the remote host is vulnerable to command injection.

Description

The remote host is running a version of Bash that is vulnerable to command injection via environment variable manipulation. Depending on the configuration of the system, an attacker could remotely execute arbitrary code.

See Also

http://seclists.org/oss-sec/2014/q3/650
http://www.nessus.org/u?dacf7829
https://www.invisiblethreat.ca/post/shellshock/

Solution

Update Bash.

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

BID	70103
CVE	CVE-2014-6271
XREF	EDB-ID:34765
XREF	EDB-ID:34766
XREF	IAVA:2014-A-0142
XREF	CISA-KNOWN-EXPLOITED:2022/07/28
XREF	CEA-ID:CEA-2019-0240

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/09/24, Modified: 2022/12/05

Plugin Output

tcp/22/ssh

```
Nessus was able to set the TERM environment variable used in an SSH
connection to :

() { :;}; /usr/bin/id > /tmp/nessus.1763055017

and read the output from the file :

uid=1000(sickos) gid=1000(sickos) groups=1000(sickos),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)


Note: Nessus has attempted to remove the file /tmp/nessus.1763055017
```

201429 - Canonical Ubuntu Linux SEoL (12.04.x) -

Synopsis

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

Description

According to its version, Canonical Ubuntu Linux is 12.04.x. It is, therefore, no longer maintained by its vendor or provider.

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

See Also

http://www.nessus.org/u?6c0a4182

Solution

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

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/0

```
OS : Canonical Ubuntu Linux 12.04.4 LTS, Precise Pangolin
Security End of Life : April 28, 2017
Time since Security End of Life (Est.) : >= 8 years
```

74213 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2225-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Matthew Daley reported an information leak in the floppy disk driver of the Linux kernel. An unprivileged local user could exploit this flaw to obtain potentially sensitive information from kernel memory.
(CVE-2014-1738)

Matthew Daley reported a flaw in the handling of ioctl commands by the floppy disk driver in the Linux kernel. An unprivileged local user could exploit this flaw to gain administrative privileges if the floppy disk module is loaded. (CVE-2014-1737)

A flaw was discovered in the vhost-net subsystem of the Linux kernel.
Guest OS users could exploit this flaw to cause a denial of service (host OS crash). (CVE-2014-0055)

A flaw was discovered in the handling of network packets when mergeable buffers are disabled for virtual machines in the Linux kernel. Guest OS users may exploit this flaw to cause a denial of service (host OS crash) or possibly gain privilege on the host OS.
(CVE-2014-0077)

Nikolay Aleksandrov discovered a race condition in Linux kernel's IPv4 fragment handling code. Remote attackers could exploit this flaw to cause a denial of service (system crash) or possibly have other unspecified impact. (CVE-2014-0100)

A flaw was discovered in the Linux kernel's handling of the SCTP handshake. A remote attacker could exploit this flaw to cause a denial of service (system crash). (CVE-2014-0101)

A flaw was discovered in the handling of routing information in Linux kernel's IPv6 stack. A remote attacker could exploit this flaw to cause a denial of service (memory consumption) via a flood of ICMPv6 router advertisement packets. (CVE-2014-2309)

An error was discovered in the Linux kernel's DCCP protocol support. A remote attacked could exploit this flaw to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2014-2523)

Max Sydorenko discovered a race condition in the Atheros 9k wireless driver in the Linux kernel. This race could be exploited by remote attackers to cause a denial of service (system crash). (CVE-2014-2672)

Adhemerval Zanella Neto discovered a flaw the in the Transactional Memory (TM) implementation for powerpc based machine. An unprivileged local user could exploit this flaw to cause a denial of service (system crash). (CVE-2014-2673)

An error was discovered in the Reliable Datagram Sockets (RDS) protocol stack in the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) or possibly have unspecified other impact. (CVE-2014-2678)

Yaara Rozenblum discovered a race condition in the Linux kernel's Generic IEEE 802.11 Networking Stack (mac80211). Remote attackers could exploit this flaw to cause a denial of service (system crash).
(CVE-2014-2706)

A flaw was discovered in the Linux kernel's ping sockets. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or possibly gain privileges via a crafted application. (CVE-2014-2851).

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

See Also

https://usn.ubuntu.com/2225-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65943
BID	66095
BID	66279
BID	66441
BID	66477
BID	66492
BID	66543
BID	66591
BID	66678
BID	66779
BID	67300
BID	67302
CVE	CVE-2014-0055
CVE	CVE-2014-0077
CVE	CVE-2014-0100
CVE	CVE-2014-0101
CVE	CVE-2014-1737
CVE	CVE-2014-1738
CVE	CVE-2014-2309
CVE	CVE-2014-2523
CVE	CVE-2014-2672
CVE	CVE-2014-2673
CVE	CVE-2014-2678
CVE	CVE-2014-2706
CVE	CVE-2014-2851
XREF	USN:2225-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/05/28, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-22.38~precise1


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.
```

106097 - MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU) -

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.59. It is, therefore, affected by multiple vulnerabilities as noted in the January 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-59.html
http://www.nessus.org/u?ae82f1b1
http://www.nessus.org/u?17a0bb67

Solution

Upgrade to MySQL version 5.5.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	102495
BID	102706
BID	102678
BID	102681
BID	102682
BID	102713
CVE	CVE-2018-2562
CVE	CVE-2018-2622
CVE	CVE-2018-2640
CVE	CVE-2018-2665
CVE	CVE-2018-2668

Plugin Information

Published: 2018/01/17, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.46-0ubuntu0.12.04.2
Fixed version : 5.5.59
```

118233 - MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU) -

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.62. It is, therefore, affected by multiple vulnerabilities as noted in the October 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-62.html
http://www.nessus.org/u?705136d8

Solution

Upgrade to MySQL version 5.5.62 or later.

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-2016-9843
CVE	CVE-2018-3133
CVE	CVE-2018-3174
CVE	CVE-2018-3282

Plugin Information

Published: 2018/10/19, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.46-0ubuntu0.12.04.2
Fixed version : 5.5.62
```

73181 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : ca-certificates update (USN-2154-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 20130906 package.

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

See Also

https://usn.ubuntu.com/2154-1/

Solution

Update the affected ca-certificates package.

Risk Factor

High

References

XREF	USN:2154-1

Plugin Information

Published: 2014/03/25, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : ca-certificates_20111211
- Fixed package : ca-certificates_20130906ubuntu0.12.04.1
```

72798 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3 vulnerability (USN-2125-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Ryan Smith-Roberts discovered that Python incorrectly handled buffer sizes when using the socket.recvfrom_into() function. An attacker could possibly use this issue to cause Python to crash, resulting in denial of service, or possibly execute arbitrary code.

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

See Also

https://usn.ubuntu.com/2125-1/

Solution

Update the affected packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65379
CVE	CVE-2014-1912
XREF	USN:2125-1

Plugin Information

Published: 2014/03/04, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : python2.7_2.7.3-0ubuntu3.4
- Fixed package : python2.7_2.7.3-0ubuntu3.5

- Installed package : python2.7-minimal_2.7.3-0ubuntu3.4
- Fixed package : python2.7-minimal_2.7.3-0ubuntu3.5
```

72366 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : perl vulnerability (USN-2099-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that Perl's Locale::Maketext module incorrectly handled backslashes and fully qualified method names. An attacker could possibly use this flaw to execute arbitrary code when an application used untrusted templates.

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

See Also

https://usn.ubuntu.com/2099-1/

Solution

Update the affected perl-modules package.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	56950
CVE	CVE-2012-6329
XREF	USN:2099-1

Exploitable With

(true) Metasploit (true)

Plugin Information

Published: 2014/02/06, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : perl-modules_5.14.2-6ubuntu2.3
- Fixed package : perl-modules_5.14.2-6ubuntu2.4
```

73402 - Ubuntu 12.04 LTS / 12.10 / 13.10 : openssl vulnerabilities (USN-2165-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Neel Mehta discovered that OpenSSL incorrectly handled memory in the TLS heartbeat extension. An attacker could use this issue to obtain up to 64k of memory contents from the client or server, possibly leading to the disclosure of private keys and other sensitive information.
(CVE-2014-0160)

Yuval Yarom and Naomi Benger discovered that OpenSSL incorrectly handled timing during swap operations in the Montgomery ladder implementation. An attacker could use this issue to perform side-channel attacks and possibly recover ECDSA nonces.
(CVE-2014-0076).

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66363
CVE	CVE-2014-0076
CVE	CVE-2014-0160
XREF	USN:2165-1
XREF	CISA-KNOWN-EXPLOITED:2022/05/25

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/04/08, Modified: 2022/05/05

Plugin Output

tcp/0

```
- Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
- Fixed package : libssl1.0.0_1.0.1-4ubuntu5.12
```

73180 - Ubuntu 12.04 LTS / 12.10 : initramfs-tools vulnerability (USN-2153-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Kees Cook discovered that initramfs-tools incorrectly mounted /run without the noexec option, contrary to expected behaviour.

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

See Also

https://usn.ubuntu.com/2153-1/

Solution

Update the affected initramfs-tools package.

Risk Factor

High

References

XREF	USN:2153-1

Plugin Information

Published: 2014/03/25, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : initramfs-tools_0.99ubuntu13.4
- Fixed package : initramfs-tools_0.99ubuntu13.5
```

100265 - Ubuntu 12.04 LTS : FreeType vulnerabilities (USN-3282-2) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, resulting in a denial of service, or possibly execute arbitrary code.

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

Solution

Update the affected libfreetype6 package.

Risk Factor

High

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-2017-8105
CVE	CVE-2017-8287
XREF	USN:3282-2

Plugin Information

Published: 2017/05/18, Modified: 2023/01/17

Plugin Output

tcp/0

```
- Installed package : libfreetype6_2.4.8-1ubuntu2.3
- Fixed package : libfreetype6_2.4.8-1ubuntu2.6
```

101148 - Ubuntu 12.04 LTS : eglibc vulnerability (USN-3323-2) (Stack Clash) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3323-1 fixed a vulnerability in the GNU C Library. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that the GNU C library did not properly handle memory when processing environment variables for setuid programs. A local attacker could use this in combination with another vulnerability to gain administrative privileges.

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

Solution

Update the affected libc6 package. Note that the updated package may not be immediately available from the package repository or its mirrors.

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-2017-1000366
XREF	USN:3323-2

Plugin Information

Published: 2017/06/30, Modified: 2025/04/02

Plugin Output

tcp/0

```
- Installed package : libc6_2.15-0ubuntu10.12
- Fixed package : libc6_2.15-0ubuntu10.20
```

100919 - Ubuntu 12.04 LTS : libnl3 vulnerability (USN-3311-2) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3311-1 fixed a vulnerability in libnl. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that libnl incorrectly handled memory when performing certain operations. A local attacker could possibly use this issue to cause libnl to crash, resulting in a denial of service, or execute arbitrary code.

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

Solution

Update the affected libnl-3-200 package. Note that the updated package may not be immediately available from the package repository and its mirrors.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2017-0553
XREF	USN:3311-2

Plugin Information

Published: 2017/06/20, Modified: 2023/01/17

Plugin Output

tcp/0

```
- Installed package : libnl-3-200_3.2.3-2ubuntu2
- Fixed package : libnl-3-200_3.2.3-2ubuntu2.1
```

72576 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2113-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Saran Neti reported a flaw in the ipv6 UDP Fragmentation Offload (UFI) in the Linux kernel. A remote attacker could exploit this flaw to cause a denial of service (panic). (CVE-2013-4563)

Mathy Vanhoef discovered an error in the the way the ath9k driver was handling the BSSID masking. A remote attacker could exploit this error to discover the original MAC address after a spoofing atack.
(CVE-2013-4579)

Andrew Honig reported a flaw in the Linux Kernel's kvm_vm_ioctl_create_vcpu function of the Kernel Virtual Machine (KVM) subsystem. A local user could exploit this flaw to gain privileges on the host machine. (CVE-2013-4587)

Andrew Honig reported a flaw in the apic_get_tmcct function of the Kernel Virtual Machine (KVM) subsystem if the Linux kernel. A guest OS user could exploit this flaw to cause a denial of service or host OS system crash. (CVE-2013-6367)

Andrew Honig reported an error in the Linux Kernel's Kernel Virtual Machine (KVM) VAPIC synchronization operation. A local user could exploit this flaw to gain privileges or cause a denial of service (system crash). (CVE-2013-6368)

Lars Bull discovered a flaw in the recalculate_apic_map function of the Kernel Virtual Machine (KVM) subsystem in the Linux kernel. A guest OS user could exploit this flaw to cause a denial of service (host OS crash). (CVE-2013-6376)

Nico Golde and Fabian Yamaguchi reported buffer underflow errors in the implementation of the XFS filesystem in the Linux kernel. A local user with CAP_SYS_ADMIN could exploit these flaw to cause a denial of service (memory corruption) or possibly other unspecified issues.
(CVE-2013-6382)

A flaw was discovered in the ipv4 ping_recvmsg function of the Linux kernel. A local user could exploit this flaw to cause a denial of service (NULL pointer dereference and system crash). (CVE-2013-6432)

mpd reported an information leak in the recvfrom, recvmmsg, and recvmsg system calls in the Linux kernel. An unprivileged local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7263)

mpb reported an information leak in the Layer Two Tunneling Protocol (l2tp) of the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7264)

mpb reported an information leak in the Phone Network protocol (phonet) in the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7265)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with ISDN sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7266)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with apple talk sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7267)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with ipx protocol sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7268)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with the netrom address family in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7269)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with packet address family sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7270)

An information leak was discovered in the recvfrom, recvmmsg, and recvmsg systemcalls when used with x25 protocol sockets in the Linux kernel. A local user could exploit this leak to obtain potentially sensitive information from kernel memory. (CVE-2013-7271)

mpb reported an information leak in the Low-Rate Wireless Personal Area Networks support (IEEE 802.15.4) in the Linux kernel. A local user could exploit this flaw to obtain sensitive information from kernel stack memory. (CVE-2013-7281)

halfdog reported an error in the AMD K7 and K8 platform support in the Linux kernel. An unprivileged local user could exploit this flaw on AMD based systems to cause a denial of service (task kill) or possibly gain privileges via a crafted application. (CVE-2014-1438)

An information leak was discovered in the Linux kernel's hamradio YAM driver for AX.25 packet radio. A local user with the CAP_NET_ADMIN capability could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-1446).

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

See Also

https://usn.ubuntu.com/2113-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2013-4563
CVE	CVE-2013-4579
CVE	CVE-2013-4587
CVE	CVE-2013-6367
CVE	CVE-2013-6368

CVE	CVE-2013-6376
CVE	CVE-2013-6382
CVE	CVE-2013-6432
CVE	CVE-2013-7263
CVE	CVE-2013-7264
CVE	CVE-2013-7265
CVE	CVE-2013-7266
CVE	CVE-2013-7267
CVE	CVE-2013-7268
CVE	CVE-2013-7269
CVE	CVE-2013-7270
CVE	CVE-2013-7271
CVE	CVE-2013-7281
CVE	CVE-2014-1438
CVE	CVE-2014-1446
XREF	USN:2113-1

Plugin Information

Published: 2014/02/19, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-17.31~precise1


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.
```

73726 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2177-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

A flaw was discovered in the Kernel Virtual Machine (KVM) subsystem of the Linux kernel. A guest OS user could exploit this flaw to execute arbitrary code on the host OS. (CVE-2014-0049)

Al Viro discovered an error in how CIFS in the Linux kernel handles uncached write operations. An unprivileged local user could exploit this flaw to cause a denial of service (system crash), obtain sensitive information from kernel memory, or possibly gain privileges.
(CVE-2014-0069).

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

See Also

https://usn.ubuntu.com/2177-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

CVSS v2.0 Base Score

7.4 (CVSS2#AV:A/AC:M/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

6.4 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	65588
BID	65909
CVE	CVE-2014-0049
CVE	CVE-2014-0069

XREF	USN:2177-1

Plugin Information

Published: 2014/04/27, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-20.34~precise1


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.
```

74359 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2239-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Pinkie Pie discovered a flaw in the Linux kernel's futex subsystem. An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or gain administrative privileges.
(CVE-2014-3153)

A flaw was discovered in the Linux kernel virtual machine's (kvm) validation of interrupt requests (irq). A guest OS user could exploit this flaw to cause a denial of service (host OS crash).
(CVE-2014-0155)

An information leak was discovered in the netfilter subsystem of the Linux kernel. An attacker could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-2568)

Sasha Levin reported a bug in the Linux kernel's virtual memory management subsystem. An unprivileged local user could exploit this flaw to cause a denial of service (system crash). (CVE-2014-3122).

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

See Also

https://usn.ubuntu.com/2239-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

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-2014-0155
CVE	CVE-2014-2568
CVE	CVE-2014-3122
CVE	CVE-2014-3153
XREF	USN:2239-1
XREF	CISA-KNOWN-EXPLOITED:2022/06/15

Exploitable With

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

Plugin Information

Published: 2014/06/06, Modified: 2022/05/25

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-23.40~precise1


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.
```

76566 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2287-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sasha Levin reported a flaw in the Linux kernel's point-to-point protocol (PPP) when used with the Layer Two Tunneling Protocol (L2TP).
A local user could exploit this flaw to gain administrative privileges. (CVE-2014-4943)

Michael S. Tsirkin discovered an information leak in the Linux kernel's segmentation of skbs when using the zerocopy feature of vhost-net. A local attacker could exploit this flaw to gain potentially sensitive information from kernel memory. (CVE-2014-0131)

An flaw was discovered in the Linux kernel's audit subsystem when auditing certain syscalls. A local attacker could exploit this flaw to obtain potentially sensitive single-bit values from kernel memory or cause a denial of service (OOPS). (CVE-2014-3917)

A flaw was discovered in the Linux kernel's implementation of user namespaces with respect to inode permissions. A local user could exploit this flaw by creating a user namespace to gain administrative privileges. (CVE-2014-4014)

Don Bailey discovered a flaw in the LZO decompress algorithm used by the Linux kernel. An attacker could exploit this flaw to cause a denial of service (memory corruption or OOPS). (CVE-2014-4608)

Don Bailey and Ludvig Strigeus discovered an integer overflow in the Linux kernel's implementation of the LZ4 decompression algorithm, when used by code not complying with API limitations. An attacker could exploit this flaw to cause a denial of service (memory corruption) or possibly other unspecified impact. (CVE-2014-4611).

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

See Also

https://usn.ubuntu.com/2287-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66101
BID	67699
BID	67988
BID	68214
BID	68218
BID	68683
CVE	CVE-2014-0131
CVE	CVE-2014-3917

CVE	CVE-2014-4014
CVE	CVE-2014-4608
CVE	CVE-2014-4611
CVE	CVE-2014-4943
XREF	USN:2287-1

Exploitable With

CANVAS (true)

Plugin Information

Published: 2014/07/17, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-26.45~precise1


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.
```

78040 - Ubuntu 12.04 LTS : openssl update (USN-2367-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

For compatibility reasons, OpenSSL in Ubuntu 12.04 LTS disables TLSv1.2 by default when being used as a client. When forcing the use of TLSv1.2, another compatibility feature (OPENSSL_MAX_TLS1_2_CIPHER_LENGTH) was used that would truncate the cipher list. This would prevent certain ciphers from being selected, and would prevent secure renegotiations. This update removes the cipher list truncation workaround when forcing the use of TLSv1.2.

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

See Also

https://usn.ubuntu.com/2367-1/

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

References

XREF	USN:2367-1

Plugin Information

Published: 2014/10/03, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
- Fixed package : libssl1.0.0_1.0.1-4ubuntu5.18
```

83413 - Ubuntu 12.04 LTS : openssl update (USN-2606-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

For compatibility reasons, Ubuntu 12.04 LTS shipped OpenSSL with TLSv1.2 disabled when being used as a client.

This update re-enables TLSv1.2 by default now that the majority of problematic sites have been updated to fix compatibility issues.

For problematic environments, TLSv1.2 can be disabled again by setting the OPENSSL_NO_CLIENT_TLS1_2 environment variable before library initialization.

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

See Also

https://usn.ubuntu.com/2606-1/

Solution

Update the affected libssl1.0.0 package.

Risk Factor

High

References

XREF USN:2606-1

Plugin Information

Published: 2015/05/13, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
- Fixed package : libssl1.0.0_1.0.1-4ubuntu5.27
```

102814 - Ubuntu 12.04 LTS : python-crypto vulnerability (USN-3199-3) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

USN-3199-1 fixed a vulnerability in Python Crypto. This update provides the corresponding update for Ubuntu 12.04 ESM.

It was discovered that the ALGnew function in block_templace.c in the Python Cryptography Toolkit contained a heap-based buffer overflow vulnerability. A remote attacker could use this flaw to execute arbitrary code by using a crafted initialization vector parameter.

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

See Also

https://usn.ubuntu.com/3199-3/

Solution

Update the affected python-crypto and / or python3-crypto 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-2013-7459
XREF	USN:3199-3

Plugin Information

Published: 2017/08/29, Modified: 2023/01/12

Plugin Output

tcp/0

```
- Installed package : python-crypto_2.4.1-1ubuntu0.1
- Fixed package : python-crypto_2.4.1-1ubuntu0.2
```

100379 - Ubuntu 12.04 LTS : rtmpdump vulnerabilities (USN-3283-2) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Dave McDaniel discovered that rtmpdump incorrectly handled certain malformed streams. If a user were tricked into processing a specially crafted stream, a remote attacker could cause rtmpdump to crash, resulting in a denial of service, or possibly execute arbitrary code.

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

Solution

Update the affected librtmp0 package. Note that the updated packages may not be immediately available from the package repository and its mirrors.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE-2015-8270
CVE	CVE-2015-8271
CVE	CVE-2015-8272
XREF	USN:3283-2

Plugin Information

Published: 2017/05/24, Modified: 2023/01/17

Plugin Output

tcp/0

```
- Installed package : librtmp0_2.4~20110711.gitc28f1bab-1
- Fixed package : librtmp0_2.4~20110711.gitc28f1bab-1ubuntu0.1
```

109166 - MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU) -

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.60. It is, therefore, affected by multiple vulnerabilities as noted in the April 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-60.html
http://www.nessus.org/u?76507bf8
http://www.nessus.org/u?64303a9a

Solution

Upgrade to MySQL version 5.5.60 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	103778
BID	103802
BID	103804
BID	103814
BID	103824
BID	103828
BID	103830
CVE	CVE-2018-2755
CVE	CVE-2018-2758
CVE	CVE-2018-2761
CVE	CVE-2018-2766
CVE	CVE-2018-2771
CVE	CVE-2018-2773
CVE	CVE-2018-2781
CVE	CVE-2018-2782
CVE	CVE-2018-2784
CVE	CVE-2018-2787
CVE	CVE-2018-2805
CVE	CVE-2018-2813
CVE	CVE-2018-2817
CVE	CVE-2018-2818
CVE	CVE-2018-2819

Plugin Information

Published: 2018/04/19, Modified: 2024/10/30

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.46-0ubuntu0.12.04.2
Fixed version : 5.5.60
```

111153 - MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU) -

Synopsis

The remote database server is affected by multiple vulnerabilities.

Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.61. It is, therefore, affected by multiple vulnerabilities as noted in the July 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

See Also

https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-61.html
http://www.nessus.org/u?50f36723

Solution

Upgrade to MySQL version 5.5.61 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	103954
BID	104766
BID	104779
BID	104786
CVE	CVE-2018-2767
CVE	CVE-2018-3058
CVE	CVE-2018-3063
CVE	CVE-2018-3066
CVE	CVE-2018-3070
CVE	CVE-2018-3081

Plugin Information

Published: 2018/07/20, Modified: 2021/05/21

Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.46-0ubuntu0.12.04.2
Fixed version : 5.5.61
```

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 : 5.5.46-0ubuntu0.12.04.2
Fixed version : 5.7.30
```

90317 - SSH Weak Algorithms Supported -

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

arcfour
arcfour128
arcfour256

The following weak client-to-server encryption algorithms are supported :

arcfour
arcfour128
arcfour256
```

73514 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Steve Holme discovered that libcurl incorrectly reused wrong connections when using protocols other than HTTP and FTP. This could lead to the use of unintended credentials, possibly exposing sensitive information. (CVE-2014-0138)

Richard Moore discovered that libcurl incorrectly validated wildcard SSL certificates that contain literal IP addresses. An attacker could possibly exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.
(CVE-2014-0139).

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

See Also

https://usn.ubuntu.com/2167-1/

Solution

Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.

Risk Factor

Medium

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

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

References

BID	66457
BID	66458
CVE	CVE-2014-0138
CVE	CVE-2014-0139
XREF	USN:2167-1

Plugin Information

Published: 2014/04/15, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libcurl3_7.22.0-3ubuntu4.7
- Fixed package : libcurl3_7.22.0-3ubuntu4.8

- Installed package : libcurl3-gnutls_7.22.0-3ubuntu4.7
- Fixed package : libcurl3-gnutls_7.22.0-3ubuntu4.8
```

72720 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerabilities (USN-2123-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that file incorrectly handled Composite Document files. An attacker could use this issue to cause file to crash, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS and Ubuntu 12.04 LTS. (CVE-2012-1571)

Bernd Melchers discovered that file incorrectly handled indirect offset values. An attacker could use this issue to cause file to consume resources or crash, resulting in a denial of service.
(CVE-2014-1943).

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

See Also

https://usn.ubuntu.com/2123-1/

Solution

Update the affected file and / or libmagic1 packages.

Risk Factor

Medium

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

BID	52225
BID	65596
CVE	CVE-2012-1571
CVE	CVE-2014-1943
XREF	USN:2123-1

Plugin Information

Published: 2014/02/27, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : file_5.09-2
- Fixed package : file_5.09-2ubuntu0.2

- Installed package : libmagic1_5.09-2
- Fixed package : libmagic1_5.09-2ubuntu0.2
```

73399 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that file incorrectly handled PE executable files.
An attacker could use this issue to cause file to crash, resulting in a denial of service.

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

See Also

https://usn.ubuntu.com/2162-1/

Solution

Update the affected file and / or libmagic1 packages.

Risk Factor

Medium

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

BID	66002
CVE	CVE-2014-2270
XREF	USN:2162-1

Plugin Information

Published: 2014/04/08, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : file_5.09-2
- Fixed package : file_5.09-2ubuntu0.3

- Installed package : libmagic1_5.09-2
- Fixed package : libmagic1_5.09-2ubuntu0.3
```

72812 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Nikos Mavrogiannopoulos discovered that GnuTLS incorrectly handled certificate verification functions. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited with specially crafted certificates to view sensitive information.

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

See Also

https://usn.ubuntu.com/2127-1/

Solution

Update the affected libgnutls26 package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

CVE	CVE-2014-0092
XREF	USN:2127-1

Plugin Information

Published: 2014/03/05, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : libgnutls26_2.12.14-5ubuntu3.5
  - Fixed package : libgnutls26_2.12.14-5ubuntu3.7
```

73202 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2155-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Jann Horn discovered that OpenSSH incorrectly handled wildcards in AcceptEnv lines. A remote attacker could use this issue to possibly bypass certain intended environment variable restrictions.

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

See Also

https://usn.ubuntu.com/2155-1/

Solution

Update the affected openssh-server package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66355
CVE	CVE-2014-2532
XREF	USN:2155-1

Plugin Information

Published: 2014/03/26, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : openssh-server_1:5.9p1-5ubuntu1.1
  - Fixed package : openssh-server_1:5.9p1-5ubuntu1.2
```

73016 - Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Sebastien Macke discovered that Sudo incorrectly handled blacklisted environment variables when the env_reset option was disabled. A local attacker could use this issue to possibly run unintended commands by using blacklisted environment variables. In a default Ubuntu installation, the env_reset option is enabled by default. This issue only affected Ubuntu 10.04 LTS and Ubuntu 12.04 LTS. (CVE-2014-0106)

It was discovered that the Sudo init script set a date in the past on existing timestamp files instead of using epoch to invalidate them completely. A local attacker could possibly modify the system time to attempt to reuse timestamp files. This issue only applied to Ubuntu 12.04 LTS, Ubuntu 12.10 and Ubuntu 13.10. (LP: #1223297).

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

See Also

https://usn.ubuntu.com/2146-1/

Solution

Update the affected sudo and / or sudo-ldap packages.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65997
CVE	CVE-2014-0106
XREF	USN:2146-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/03/14, Modified: 2021/01/19

Plugin Output

tcp/0

```
  - Installed package : sudo_1.8.3p1-1ubuntu3.4
  - Fixed package : sudo_1.8.3p1-1ubuntu3.6
```

72701 - Ubuntu 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2121-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Suman Jana discovered that GnuTLS incorrectly handled version 1 intermediate certificates. This resulted in them being considered to be a valid CA certificate by default, which was contrary to documented behaviour.

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

See Also

https://usn.ubuntu.com/2121-1/

Solution

Update the affected libgnutls26 package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	65559
CVE	CVE-2014-1959
XREF	USN:2121-1

Plugin Information

Published: 2014/02/26, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : libgnutls26_2.12.14-5ubuntu3.5
- Fixed package : libgnutls26_2.12.14-5ubuntu3.6
```

73401 - Ubuntu 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2164-1)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Matthew Vernon discovered that OpenSSH did not correctly check SSHFP DNS records if a server presented an unacceptable host certificate. A malicious server could use this issue to disable SSHFP checking.

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

See Also

https://usn.ubuntu.com/2164-1/

Solution

Update the affected openssh-client package.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	66459
CVE	CVE-2014-2653
XREF	USN:2164-1

Plugin Information

Published: 2014/04/08, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : openssh-client_1:5.9p1-5ubuntu1.1
- Fixed package : openssh-client_1:5.9p1-5ubuntu1.3
```

97936 - Ubuntu 12.04 LTS : eglibc regression (USN-3239-3)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-3239-1 fixed vulnerabilities in the GNU C Library. Unfortunately, the fix for CVE-2016-3706 introduced a regression that in some circumstances prevented IPv6 addresses from resolving. This update reverts the change in Ubuntu 12.04 LTS. We apologize for the error.

It was discovered that the GNU C Library incorrectly handled the strxfrm() function. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8982)

It was discovered that an integer overflow existed in the
_IO_wstr_overflow() function of the GNU C Library. An attacker could use this to cause a denial of service or possibly execute arbitrary code. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8983)

It was discovered that the fnmatch() function in the GNU C Library did not properly handle certain malformed patterns.
An attacker could use this to cause a denial of service.
This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2015-8984)

Alexander Cherepanov discovered a stack-based buffer overflow in the glob implementation of the GNU C Library. An attacker could use this to specially craft a directory layout and cause a denial of service. (CVE-2016-1234)

Michael Petlan discovered an unbounded stack allocation in the getaddrinfo() function of the GNU C Library. An attacker could use this to cause a denial of service. (CVE-2016-3706)

Aldy Hernandez discovered an unbounded stack allocation in the sunrpc implementation in the GNU C Library. An attacker could use this to cause a denial of service. (CVE-2016-4429)

Tim Ruehsen discovered that the getaddrinfo() implementation in the GNU C Library did not properly track memory allocations. An attacker could use this to cause a denial of service. This issue only affected Ubuntu 16.04 LTS.
(CVE-2016-5417)

Andreas Schwab discovered that the GNU C Library on ARM 32-bit platforms did not properly set up execution contexts.
An attacker could use this to cause a denial of service.
(CVE-2016-6323).

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

See Also

https://usn.ubuntu.com/3239-3/

Solution

Update the affected libc6 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

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-8982
CVE	CVE-2015-8983
CVE	CVE-2015-8984
CVE	CVE-2016-1234
CVE	CVE-2016-3706
CVE	CVE-2016-4429
CVE	CVE-2016-5417
CVE	CVE-2016-6323
XREF	USN:3239-3

Plugin Information

Published: 2017/03/24, Modified: 2023/01/12

Plugin Output

tcp/0

```
- Installed package : libc6_2.15-0ubuntu10.12
- Fixed package : libc6_2.15-0ubuntu10.18
```

72900 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2137-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

An information leak was discovered in the Linux kernel when built with the NetFilter Connection Tracking (NF_CONNTRACK) support for IRC protocol (NF_NAT_IRC). A remote attacker could exploit this flaw to obtain potentially sensitive kernel information when communicating over a client- to-client IRC connection(/dcc) via a NAT-ed network.
(CVE-2014-1690)

Matthew Thode reported a denial of service vulnerability in the Linux kernel when SELinux support is enabled. A local user with the CAP_MAC_ADMIN capability (and the SELinux mac_admin permission if running in enforcing mode) could exploit this flaw to cause a denial of service (kernel crash). (CVE-2014-1874)

An information leak was discovered in the Linux kernel's NFS filesystem. A local users with write access to an NFS share could exploit this flaw to obtain potential sensative information from kernel memory. (CVE-2014-2038).

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

See Also

https://usn.ubuntu.com/2137-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

CVSS v2.0 Base Score

4.4 (CVSS2#AV:L/AC:M/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

References

BID	65180
BID	65688
CVE	CVE-2014-1690
CVE	CVE-2014-1874
CVE	CVE-2014-2038
XREF	USN:2137-1

Plugin Information

Published: 2014/03/10, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-18.32~precise1

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.
```

76296 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2261-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Salva Peiro discovered an information leak in the Linux kernel's media- device driver. A local attacker could exploit this flaw to obtain sensitive information from kernel memory. (CVE-2014-1739)

A bounds check error was discovered in the socket filter subsystem of the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) via crafted BPF instructions.
(CVE-2014-3144)

A remainder calculation error was discovered in the socket filter subsystem of the Linux kernel. A local user could exploit this flaw to cause a denial of service (system crash) via crafted BPF instructions.
(CVE-2014-3145).

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

See Also

https://usn.ubuntu.com/2261-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

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

BID	67309
BID	67321
BID	68048
CVE	CVE-2014-1739
CVE	CVE-2014-3144
CVE	CVE-2014-3145
XREF	USN:2261-1

Plugin Information

Published: 2014/06/28, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-24.41~precise1


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.
```

73890 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2201-1) -

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

A flaw was discovered in the Linux kernel's pseudo tty (pty) device.
An unprivileged user could exploit this flaw to cause a denial of service (system crash) or potentially gain administrator privileges.

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

See Also

https://usn.ubuntu.com/2201-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

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

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

References

BID	67199
CVE	CVE-2014-0196
XREF	USN:2201-1
XREF	CISA-KNOWN-EXPLOITED:2023/06/02

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2014/05/06, Modified: 2023/05/14

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-20.35~precise1


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.
```

76383 - Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2271-1)

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

Andy Lutomirski discovered a flaw with the Linux kernel's ptrace syscall on x86_64 processors. An attacker could exploit this flaw to cause a denial of service (System Crash) or potential gain administrative privileges.

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

See Also

https://usn.ubuntu.com/2271-1/

Solution

Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

Risk Factor

Medium

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

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

References

BID	68411
CVE	CVE-2014-4699
XREF	USN:2271-1

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/07/06, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : linux-image-3.11.0-15-generic_3.11.0-15.25~precise1
- Fixed package : linux-image-3.11.0-<ANY>-generic_3.11.0-24.42~precise1


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.
```

87815 - Ubuntu 12.04 LTS : openssl vulnerability (USN-2863-1) (SLOTH)

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Karthikeyan Bhargavan and Gaetan Leurent discovered that OpenSSL incorrectly allowed MD5 to be used for TLS 1.2 connections. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could be exploited to view sensitive information.

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

See Also

https://usn.ubuntu.com/2863-1/

Solution

Update the affected libssl1.0.0 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: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:N/I:P/A:N)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-7575
XREF	USN:2863-1

Plugin Information

Published: 2016/01/08, Modified: 2023/01/17

Plugin Output

tcp/0

```
- Installed package : libssl1.0.0_1.0.1-4ubuntu5.11
- Fixed package : libssl1.0.0_1.0.1-4ubuntu5.33
```

90021 - Ubuntu 12.04 LTS : pam regression (USN-2935-3) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

USN-2935-1 fixed vulnerabilities in PAM. The updates contained a packaging change that prevented upgrades in certain multiarch environments. USN-2935-2 intended to fix the problem but was incomplete for Ubuntu 12.04 LTS. This update fixes the problem in Ubuntu 12.04 LTS.

We apologize for the inconvenience.

It was discovered that the PAM pam_userdb module incorrectly used a case-insensitive method when comparing hashed passwords. A local attacker could possibly use this issue to make brute-force attacks easier. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2013-7041)

Sebastian Krahmer discovered that the PAM pam_timestamp module incorrectly performed filtering. A local attacker could use this issue to create arbitrary files, or possibly bypass authentication. This issue only affected Ubuntu 12.04 LTS and Ubuntu 14.04 LTS. (CVE-2014-2583)

Sebastien Macke discovered that the PAM pam_unix module incorrectly handled large passwords. A local attacker could possibly use this issue in certain environments to enumerate usernames or cause a denial of service. (CVE-2015-3238).

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

See Also

https://usn.ubuntu.com/2935-3/

Solution

Update the affected libpam-modules package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2013-7041
CVE	CVE-2014-2583
CVE	CVE-2015-3238

XREF USN:2935-3

Plugin Information

Published: 2016/03/18, Modified: 2023/01/12

Plugin Output

tcp/0

```
- Installed package : libpam-modules_1.1.3-7ubuntu2
- Fixed package : libpam-modules_1.1.3-7ubuntu2.3
```

70658 - SSH Server CBC Mode Ciphers Enabled -

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

77526 - Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1) -

Synopsis

The remote Ubuntu host is missing a security-related patch.

Description

Daniel Genkin, Adi Shamir, and Eran Tromer discovered that GnuPG was susceptible to an adaptive chosen ciphertext attack via physical side channels. A local attacker could use this attack to possibly recover private keys.

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

See Also

https://usn.ubuntu.com/2339-1/

Solution

Update the affected gnupg package.

Risk Factor

Low

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

BID	69164
CVE	CVE-2014-5270
XREF	USN:2339-1

Plugin Information

Published: 2014/09/04, Modified: 2021/01/19

Plugin Output

tcp/0

```
- Installed package : gnupg_1.4.11-3ubuntu2.5
- Fixed package : gnupg_1.4.11-3ubuntu2.7
```

141394 - Apache HTTP Server Installed (Linux) -

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/08/19

Plugin Output

tcp/0

```
Nessus detected 4 installs of Apache:

Path : /usr/lib/apache2/mpm-worker/apache2
Version : 2.2.22
Running : no

Configs found :

Loaded modules :

Path : /usr/lib/apache2/mpm-event/apache2
Version : 2.2.22
Running : no

Configs found :

Loaded modules :

Path : /usr/lib/apache2/mpm-prefork/apache2
Version : 2.2.22
Running : no

Configs found :

Loaded modules :

Path : /usr/lib/apache2/mpm-itk/apache2
Version : 2.2.22
Running : no

Configs found :

Loaded modules :
```

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:canonical:ubuntu_linux:12.04.4::~~lts~~~ -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
cpe:/a:gnupg:libgcrypt:1.5.0 -> GnuPG Libgcrypt
cpe:/a:haxx:curl:7.22.0 -> Haxx Curl
cpe:/a:haxx:libcurl:7.22.0 -> Haxx libcurl
cpe:/a:mysql:mysql:5.5.46-0ubuntu0.12.04.2_ -> MySQL MySQL
cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:5.9p1 -> OpenBSD OpenSSH
cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:1.0.1 -> OpenSSL Project OpenSSL
cpe:/a:php:php:5.3.10 -> PHP PHP
cpe:/a:squid-cache:squid:3.1.19 -> squid-cache.org Squid
cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ
cpe:/a:vim:vim:7.3 -> Vim
```

182774 - Curl Installed (Linux / Unix) -

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/curl
Version : 7.22.0
Associated Package : curl 7.22.0-3ubuntu4.7
Managed by OS : True
```

55472 - Device Hostname -

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/07/28

Plugin Output

tcp/0

```
Hostname : SickOs
SickOs (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 :

- 10.136.108.108 (on interface eth0)
- 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH -

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

- 2409:40c0:50:80bc:a00:27ff:fec6:383f (on interface eth0)
- 2409:40c0:50:80bc:ccc4:f913:e4df:5060 (on interface eth0)
- fe80::a00:27ff:fec6:383f (on interface eth0)
- ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH -

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

- 08:00:27:c6:38:3f (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:c6:38:3f
IPv4:
- Address : 10.136.108.108
Netmask : 255.255.255.0
Broadcast : 10.136.108.255
IPv6:
- Address : 2409:40c0:50:80bc:a00:27ff:fec6:383f
Prefixlen : 64
Scope : global
- Address : 2409:40c0:50:80bc:ccc4:f913:e4df:5060
Prefixlen : 64
Scope : global
- Address : fe80::a00:27ff:fec6:383f
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:
10.136.108.228:
subnets:
- 0.0.0.0/0
ipv6_gateways:
fe80::4a2:97ff:fec8:6a88:
subnets:
```

```
- ::/0
Interface Routes:
eth0:
ipv4_subnets:
- 10.136.108.0/24
ipv6_subnets:
- 2409:40c0:50:80bc::/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/sbin
/usr/local/bin
/usr/sbin
/usr/bin
/sbin
/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:C6:38:3F : 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:C6:38:3F
```

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/3128/http_proxy

```
The remote web server type is :

squid/3.1.19
```

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/3128/http_proxy

```
Response Code : HTTP/1.0 400 Bad Request

Protocol version : HTTP/1.0
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Server: squid/3.1.19
Mime-Version: 1.0
Date: Thu, 13 Nov 2025 17:26:26 GMT
Content-Type: text/html
Content-Length: 3150
X-Squid-Error: ERR_INVALID_URL 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from localhost
X-Cache-Lookup: NONE from localhost:3128
Via: 1.0 localhost (squid/3.1.19)
Connection: close

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
/*
Stylesheet for Squid Error pages
Adapted from design by Free CSS Templates
http://www.freecsstemplates.org
Released for free under a Creative Commons Attribution 2.5 License
*/

/* Page basics */
* {
font-family: verdana, sans-serif;
}

html body {
margin: 0;
padding: 0;
background: #efefef;
font-size: 12px;
color: #1e1e1e;
}

/* Page displayed title area */
#titles {
margin-left: 15px;
padding: 10px;
padding-left: 100px;
background: url('http://www.squid-cache.org/Artwork/SN.png') no-repeat left;
}

/* initial title */
#titles h1 {
color: #000000;
}
#titles h2 {
color: #000000;
}

/* special event: FTP success page titles */
#titles ftpsuccess {
background-color:#00ff00;
width:100%;
}

/* Page displayed body content area */
#content {
padding: 10px;
background: #ffffff;
}
```

```
/* General text */
p {
}

/* error brief description */
#error p {
}

/* some data which may have caused the problem */
#data {
}

/* the error message received from the system or other software */
#sysmsg {
}

pre {
font-family:sans-serif;
}

/* special event: FTP / Gopher directory listing */
#dirmsg {
font-family: courier;
color: black;
font-size: 10pt;
}
#dirlisting {
margin-left: 2%;
margin-right: 2%;
}
#dirlisting tr.entry td.icon,td.filename,td.size,td.date {
border-bottom: groove;
}
#dirlisting td.size {
width: 50px;
text-align: right;
padding-right: 5px;
}

/* horizontal lines */
hr {
margin: 0;
}

/* page displayed footer area */
#footer {
font-size: 9px;
padding-left: 10px;
}


body
:lang(fa) { direction: rtl; font-size: 100%; font-family: Tahoma, Roya, sans-serif; float: right; }
:lang(he) { direction: rtl; }
--></style>
</head><body id=ERR_INVALID_URL>
<div id="titles">
<h1>ERROR</h1>
<h2>The requested URL could not be retrieved</h2>
</div>
<hr>

<div id="content">
<p>The following error was encountered while trying to retrieve the URL: <a href="/">/</a></p>

<blockquote id="error">
<p><b>Invalid URL</b></p>
</blockquote>

<p>Some aspect of the requested URL is incorrect.</p>

<p>Some possible problems are:</p>
<ul>
<li><p>Missing or incorrect access protocol (should be <q>http://</q> or similar)</p></li>
<li><p>Missing hostname</p></li>
<li><p>Illegal double-escape in the URL-Path</p></li>
<li><p>Illegal character in hostname; underscores are not allowed.</p></li>
</ul>

<p>Your cache administrator is <a href="mailto:webmaster?subject=CacheErrorInfo%20-
%20ERR_INVALID_URL&amp;body=CacheHost%3A%20localhost%0D%0AErrPage%3A%20ERR_INVALID_URL%0D%0AErr%3A%20%5Bnone%5D%0D%0ATimeStamp%3A%20
Thu,%2013%20Nov%202025%2017%3A26%3A26%20GMT%0D%0A%0D%0AClientIP%3A%2010.136.108.33%0D%0A%0D%0AHTTP%20Request%3A%0D%0A%0D%0A%0D%0A">w
ebmaster</a>.</p>
<br>
</div>

<hr>
<div id="footer">
<p>Generated Thu, 13 Nov 2025 17:26:26 GMT by localhost (squid/3.1.19)</p>
<!-- ERR_INVALID_URL -->
</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 : 10.136.108.108
Assign Method : static
+ IPv6
- Address : 2409:40c0:50:80bc:ccc4:f913:e4df:5060
Assign Method : dynamic
- Address : 2409:40c0:50:80bc:a00:27ff:fec6:383f
Assign Method : dynamic
- Address : fe80::a00:27ff:fec6:383f
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/i386-linux-gnu/libgcrypt.so.11
Version : 1.5.0

Path : /lib/i386-linux-gnu/libgcrypt.so.11.7.0
Version : 1.5.0
```

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 29G 1.3G 26G 5% /
udev 492M 4.0K 492M 1% /dev
tmpfs 201M 276K 200M 1% /run
none 5.0M 0 5.0M 0% /run/lock
none 501M 0 501M 0% /run/shm


$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 30G 0 disk
├─sda1 8:1 0 29G 0 part /
├─sda2 8:2 0 1K 0 part
└─sda5 8:5 0 1022M 0 part [SWAP]


$ mount -l
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
```

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: IST +0530
Via /etc/timezone: Asia/Calcutta
Via /etc/localtime: IST-5:30
```

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 : sickos
Home folder : /home/sickos
Start script : /bin/bash
Groups : lpadmin
cdrom
sickos
sambashare
sudo
plugdev
dip
adm

----------[ System Accounts ]----------

User : root
Home folder : /root
Start script : /bin/bash
Groups : root

User : daemon
Home folder : /usr/sbin
Start script : /bin/sh
Groups : daemon

User : bin
Home folder : /bin
Start script : /bin/sh
Groups : bin

User : sys
Home folder : /dev
Start script : /bin/sh
Groups : sys

User : sync
Home folder : /bin
Start script : /bin/sync
Groups : nogroup

User : games
Home folder : /usr/games
Start script : /bin/sh
Groups : games

User : man
Home folder : /var/cache/man
Start script : /bin/sh
Groups : man

User : lp
Home folder : /var/spool/lpd
Start script : /bin/sh
Groups : lp

User : mail
Home folder : /var/mail
```

```
Start script : /bin/sh
Groups : mail

User : news
Home folder : /var/spool/news
Start script : /bin/sh
Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /bin/sh
Groups : uucp

User : proxy
Home folder : /bin
Start script : /bin/sh
Groups : proxy

User : www-data
Home folder : /var/www
Start script : /bin/sh
Groups : www-data

User : backup
Home folder : /var/backups
Start script : /bin/sh
Groups : backup

User : list
Home folder : /var/list
Start script : /bin/sh
Groups : list

User : irc
Home folder : /var/run/ircd
Start script : /bin/sh
Groups : irc

User : gnats
Home folder : /var/lib/gnats
Start script : /bin/sh
Groups : gnats

User : nobody
Home folder : /nonexistent
Start script : /bin/sh
Groups : nogroup

User : libuuid
Home folder : /var/lib/libuuid
Start script : /bin/sh
Groups : libuuid

User : syslog
Home folder : /home/syslog
Start script : /bin/false
Groups : syslog

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : whoopsie
Home folder : /nonexistent
Start script : /bin/false
Groups : whoopsie

User : landscape
Home folder : /var/lib/landscape
Start script : /bin/false
Groups : landscape

User : sshd
Home folder : /var/run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql


----------[ 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 : 5.5.46-0ubuntu0.12.04.2
```

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 : SickOS 1.1
Scan policy used : Advanced Scan
Scanner IP : 10.136.108.33
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 129.492 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 'sickos' 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 : 2025/11/13 17:23 UTC
Scan duration : 519 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

```
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/3128/http_proxy

```
Port 3128/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/56892

```
Port 56892/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/60550

```
Port 60550/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 14.04 Linux Kernel 3.13
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1

Remote operating system : Linux Kernel 3.11.0-15-generic
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386 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 3.11.0-15-generic on Ubuntu 12.04
Confidence level : 100
Method : LinuxDistribution
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
HTTP:!:Server: squid/3.1.19
```

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 3.11.0-15-generic on Ubuntu 12.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 3.11.0-15-generic on Ubuntu 12.04
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) -

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
wheezy/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 15.607510 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 : sickos
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 : 5.9p1
Banner : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
```

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 : 1.0.1
Associated Package : openssl 1.0.1-4ubuntu5.11
Managed by OS : True

Path : /lib/i386-linux-gnu/libssl.so.1.0.0
Version : 1.0.1
Associated Package : libssl1.0.0

Path : /lib/i386-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/i386-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libatalla.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgmp.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
```

216936 - PHP Scripting Language Installed (Unix) -

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.
Thorough test is required to get results on hosts running MacOS.

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/07/28

Plugin Output

tcp/0

```
Path : /usr/bin/php5
Version : 5.3.10
Associated Package : php5-cli: /usr/bin/php5
INI file : /etc/php5/cli/php.ini
INI source : PHP binary grep
Managed by OS : True
```

179139 - Package Manager Packages Report (nix) -

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

```
. You need to take the following 18 actions :

[ MySQL Denial of Service (Jul 2020 CPU) (138561) ]

+ Action to take : Refer to the vendor advisory.

+Impact : Taking this action will resolve 27 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1) (73514) ]

+ Action to take : Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1) (73399) ]

+ Action to take : Update the affected file and / or libmagic1 packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1) (72812) ]

+ Action to take : Update the affected libgnutls26 package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2155-1) (73202) ]

+ Action to take : Update the affected openssh-server package.

[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3 vulnerability (USN-2125-1) (72798) ]

+ Action to take : Update the affected packages.

[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1) (73016) ]

+ Action to take : Update the affected sudo and / or sudo-ldap packages.

[ Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : perl vulnerability (USN-2099-1) (72366) ]

+ Action to take : Update the affected perl-modules package.

[ Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1) (77526) ]

+ Action to take : Update the affected gnupg package.

[ Ubuntu 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2164-1) (73401) ]

+ Action to take : Update the affected openssh-client package.

[ Ubuntu 12.04 LTS : FreeType vulnerabilities (USN-3282-2) (100265) ]

+ Action to take : Update the affected libfreetype6 package.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 12.04 LTS : eglibc vulnerability (USN-3323-2) (Stack Clash) (101148) ]

+ Action to take : Update the affected libc6 package. Note that the updated package may not be immediately available from the
package repository or its mirrors.

+Impact : Taking this action will resolve 9 different vulnerabilities (CVEs).


[ Ubuntu 12.04 LTS : libnl3 vulnerability (USN-3311-2) (100919) ]

+ Action to take : Update the affected libnl-3-200 package. Note that the updated package may not be immediately available from the
package repository and its mirrors.


[ Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2287-1) (76566) ]

+ Action to take : Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.

+Impact : Taking this action will resolve 53 different vulnerabilities (CVEs).


[ Ubuntu 12.04 LTS : openssl vulnerability (USN-2863-1) (SLOTH) (87815) ]

+ Action to take : Update the affected libssl1.0.0 package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 12.04 LTS : pam regression (USN-2935-3) (90021) ]

+ Action to take : Update the affected libpam-modules package.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 12.04 LTS : python-crypto vulnerability (USN-3199-3) (102814) ]

+ Action to take : Update the affected python-crypto and / or python3-crypto packages.


[ Ubuntu 12.04 LTS : rtmpdump vulnerabilities (USN-3283-2) (100379) ]

+ Action to take : Update the affected librtmp0 package. Note that the updated packages may not be immediately available from the
package repository and its mirrors.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

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 addresss were gathered :

- 2409:40c0:50:80bc:ccc4:f913:e4df:5060
- 2409:40c0:50:80bc:a00:27ff:fec6:383f
```

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-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-256-96
hmac-sha2-512
hmac-sha2-512-96
umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
ssh-dss
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_server_to_client :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-256-96
hmac-sha2-512
hmac-sha2-512-96
umac-64@openssh.com

The server supports the following options for kex_algorithms :

diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
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 :

3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

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 : sickos
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C dmidecode"
Response : "# dmidecode 2.11"
Error : "\n/dev/mem: Permission denied"
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 2.11"
Error : "\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 : ""
- Plugin Filename : enumerate_oci_nix.nasl
Plugin ID : 154138
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C dmidecode -s chassis-asset-tag 2>&1"
Response : "/dev/mem: Permission denied"
Error : ""
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/dev/mem: Permission denied"
Error : ""
```

```
- Plugin Filename : host_tag_nix.nbin
Plugin ID : 87414
Plugin Name : Host Tagging (Linux)
- Command : "sh -c \"echo 718ad9a812d3459cb1cb4f8d371b58c1 > /etc/tenable_tag && echo OK\""
Response : null
Error : "\nsh: 1: cannot create /etc/tenable_tag: Permission denied"
- Plugin Filename : localusers_pwexpiry.nasl
Plugin ID : 83303
Plugin Name : Unix / Linux - Local Users Information : Passwords Never Expire
- Command : "cat /etc/shadow"
Response : null
Error : "\ncat: \n/etc/shadow: Permission denied"
- Plugin Filename : ssh_get_info2.nasl
Plugin ID : 97993
Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
- Command : "lsmod | grep -q iptable_filter && iptables -L -n -v -t filter"
Response : null
Error : "\niptables v1.4.12: \ncan't initialize iptables table `filter': Permission denied (you must be root)\n\n\nPerhaps iptables
or your kernel needs to be upgraded."
- Command : "lsmod | grep -q _conntrack_ipv4 && iptables -L -n -v -t nat"
Response : null
Error : "\niptables v1.4.12: \ncan't initialize iptables table `nat': Permission denied (you must be root)\n\n\nPerhaps iptables or
your kernel needs to be upgraded."
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

```
- 1.99
- 2.0
```

90707 - SSH SCP Protocol Detection -

Synopsis

The remote host supports the SCP protocol over SSH.

Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

See Also

https://en.wikipedia.org/wiki/Secure_copy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96
```

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_5.9p1 Debian-5ubuntu1.1
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/3128/http_proxy

```
A web server is running on this port.
```

tcp/3128/http_proxy

```
An HTTP proxy 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 :

Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Description
+++-==========================================================================================-
==========================================================================================-
=================================================================================================================================
=============================================================
ii accountsservice 0.6.15-2ubuntu9.7 query and manipulate user account information
ii acpid 1:2.0.10-1ubuntu3 Advanced Configuration and Power Interface event daemon
ii adduser 3.113ubuntu2 add and remove users and groups
ii apache2 2.2.22-1ubuntu1.10 Apache HTTP Server metapackage
ii apache2-mpm-prefork 2.2.22-1ubuntu1.10 Apache HTTP Server - traditional non-threaded model
ii apache2-utils 2.2.22-1ubuntu1.10 utility programs for webservers
ii apache2.2-bin 2.2.22-1ubuntu1.10 Apache HTTP Server common binary files
ii apache2.2-common 2.2.22-1ubuntu1.10 Apache HTTP Server common files
ii apparmor 2.7.102-0ubuntu3.9 User-space parser utility for AppArmor
ii apport 2.0.1-0ubuntu17.6 automatically generate crash reports for debugging
ii apport-symptoms 0.16.1 symptom scripts for apport
ii apt 0.8.16~exp12ubuntu10.16 commandline package manager
ii apt-transport-https 0.8.16~exp12ubuntu10.16 https download transport for APT
ii apt-utils 0.8.16~exp12ubuntu10.16 package managment related utility programs
ii apt-xapian-index 0.44ubuntu5.1 maintenance and search tools for a Xapian index of Debian packages
ii aptitude 0.6.6-1ubuntu1.2 terminal-based package manager (terminal interface only)
ii at 3.1.13-1ubuntu1 Delayed job execution and batch processing
ii base-files 6.5ubuntu6.7 Debian base system miscellaneous files
ii base-passwd 3.5.24 Debian base system master password and group files
ii bash 4.2-2ubuntu2.1 GNU Bourne Again SHell
ii bash-completion 1:1.3-1ubuntu8.1 programmable completion for the bash shell
ii bc 1.06.95-2ubuntu1 The GNU bc arbitrary precision calculator language
ii bind9-host 1:9.8.1.dfsg.P1-4ubuntu0.8 Version of 'host' bundled with BIND 9.X
ii binutils 2.22-6ubuntu1.3 GNU assembler, linker and binary utilities
ii bsdmainutils 8.2.3ubuntu1 collection of more utilities from FreeBSD
ii bsdutils 1:2.20.1-1ubuntu3 Basic utilities from 4.4BSD-Lite
ii busybox-initramfs 1:1.18.5-1ubuntu4.1 Standalone shell setup for initramfs
ii busybox-static 1:1.18.5-1ubuntu4.1 Standalone rescue shell with tons of builtin utilities
ii byobu 5.17-0ubuntu1 powerful, text based window manager and shell multiplexer
```

```
ii bzip2 1.0.6-1 high-quality block-sorting file compressor - utilities
ii ca-certificates 20111211 Common CA certificates
ii command-not-found 0.2.46ubuntu6 Suggest installation of packages in interactive bash sessions
ii command-not-found-data 0.2.46ubuntu6 Set of data files for command-not-found.
ii console-setup 1.70ubuntu5 console font and keymap setup program
ii coreutils 8.13-3ubuntu3.2 GNU core utilities
ii cpio 2.11-7ubuntu3 GNU cpio -- a program to manage archives of files
ii cpp 4:4.6.3-1ubuntu5 GNU C preprocessor (cpp)
ii cpp-4.6 4.6.3-1ubuntu5 GNU C preprocessor
ii cron 3.0pl1-120ubuntu4 process scheduling daemon
ii curl 7.22.0-3ubuntu4.7 Get a file from an HTTP, HTTPS or FTP server
ii dash 0.5.7-2ubuntu2 POSIX-compliant shell
ii dbus 1.4.18-1ubuntu1.4 simple interprocess messaging system (daemon and utilities)
ii debconf 1.5.42ubuntu1 Debian configuration management system
ii debconf-i18n 1.5.42ubuntu1 full internationalization support for debconf
ii debianutils 4.2.1ubuntu2 Miscellaneous utilities specific to Debian
ii diffutils 1:3.2-1ubuntu1 File comparison utilities
ii dmidecode 2.11-4 SMBIOS/DMI table decoder
ii dmsetup 2:1.02.48-4ubuntu7.4 The Linux Kernel Device Mapper userspace library
ii dnsutils 1:9.8.1.dfsg.P1-4ubuntu0.8 Clients provided with BIND
ii dosfstools 3.0.12-1ubuntu1.1 utilities for making and checking MS-DOS FAT filesystems
ii dpkg 1.16.1.2ubuntu7.2 Debian package management system
ii e2fslibs 1.42-1ubuntu2 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.42-1ubuntu2 ext2/ext3/ext4 file system utilities
ii ed 1.5-3 classic UNIX line editor
ii eject 2.1.5+deb1+cvs20081104-9 ejects CDs and operates CD-Changers under Linux
ii file 5.09-2 Determines file type using "magic" numbers
ii findutils 4.4.2-4ubuntu1 utilities for finding files--find, xargs
ii fontconfig-config 2.8.0-3ubuntu9.1 generic font configuration library - configuration
ii fonts-ubuntu-font-family-console 0.80-0ubuntu2 Ubuntu Font Family Linux console fonts, sans-serif monospace
ii friendly-recovery 0.2.25 Make recovery more user-friendly
ii ftp 0.17-25 classical file transfer client
ii fuse 2.8.6-2ubuntu2 Filesystem in Userspace
ii gcc 4:4.6.3-1ubuntu5 GNU C compiler
ii gcc-4.6 4.6.3-1ubuntu5 GNU C compiler
ii gcc-4.6-base 4.6.3-1ubuntu5 GCC, the GNU Compiler Collection (base package)
ii geoip-database 20111220-1 IP lookup command line tools that use the GeoIP library (country database)
ii gettext-base 0.18.1.1-5ubuntu3 GNU Internationalization utilities for the base system
ii gir1.2-glib-2.0 1.32.0-1 Introspection data for GLib, GObject, Gio and GModule
ii gnupg 1.4.11-3ubuntu2.5 GNU privacy guard - a free PGP replacement
ii gpgv 1.4.11-3ubuntu2.5 GNU privacy guard - signature verification tool
ii grep 2.10-1 GNU grep, egrep and fgrep
ii groff-base 1.21-7 GNU troff text-formatting system (base system components)
ii grub-common 1.99-21ubuntu3.18 GRand Unified Bootloader (common files)
ii grub-gfxpayload-lists 0.6 GRUB gfxpayload blacklist
ii grub-pc 1.99-21ubuntu3.18 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 1.99-21ubuntu3.18 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
ii grub2-common 1.99-21ubuntu3.18 GRand Unified Bootloader (common files for version 2)
ii gzip 1.4-1ubuntu2 GNU compression utilities
ii hdparm 9.37-0ubuntu3.1 tune hard disk parameters for high performance
ii hostname 3.06ubuntu1 utility to set/show the host name or domain name
ii ifupdown 0.7~beta2ubuntu10 high level tools to configure network interfaces
ii info 4.13a.dfsg.1-8ubuntu2 Standalone GNU Info documentation browser
ii initramfs-tools 0.99ubuntu13.4 tools for generating an initramfs
ii initramfs-tools-bin 0.99ubuntu13.4 binaries used by initramfs-tools
ii initscripts 2.88dsf-13.10ubuntu11.1 scripts for initializing and shutting down the system
ii insserv 1.14.0-2.1ubuntu2 Tool to organize boot sequence using LSB init.d script dependencies
ii install-info 4.13a.dfsg.1-8ubuntu2 Manage installed documentation in info format
ii installation-report 2.46ubuntu1 system installation report
ii iproute 20111117-1ubuntu2.1 networking and traffic control tools
ii iptables 1.4.12-1ubuntu5 administration tools for packet filtering and NAT
ii iputils-ping 3:20101006-1ubuntu1 Tools to test the reachability of network hosts
ii iputils-tracepath 3:20101006-1ubuntu1 Tools to trace the network path to a remote host
ii irqbalance 0.56-1ubuntu4 Daemon to balance interrupts for SMP systems
ii isc-dhcp-client 4.1.ESV-R4-0ubuntu5.9 ISC DHCP client
ii isc-dhcp-common 4.1.ESV-R4-0ubuntu5.9 common files used by all the isc-dhcp* packages
ii iso-codes 3.31-1 ISO language, territory, currency, script codes and their translations
ii kbd 1.15.2-3ubuntu4 Linux console font and keytable utilities
ii keyboard-configuration 1.70ubuntu5 system-wide keyboard preferences
ii klibc-utils 1.5.25-1ubuntu2 small utilities built with klibc for early boot
ii krb5-locales 1.10+dfsg~beta1-2ubuntu0.3 Internationalization support for MIT Kerberos
ii landscape-common 13.07.3-0ubuntu0.12.04 The Landscape administration system client - Common files
ii language-pack-en 1:12.04+20140106 translation updates for language English
ii language-pack-en-base 1:12.04+20140106 translations for language English
ii language-selector-common 0.79.4 Language selector for Ubuntu
ii laptop-detect 0.13.7ubuntu2 attempt to detect a laptop
ii less 444-1ubuntu1 pager program similar to more
ii libaccountsservice0 0.6.15-2ubuntu9.7 query and manipulate user account information - shared libraries
ii libacl1 2.2.51-5ubuntu1 Access control list shared library
ii libapache2-mod-php5 5.3.10-1ubuntu3.21 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapr1 1.4.6-1 Apache Portable Runtime Library
ii libaprutil1 1.3.12+dfsg-3 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.3.12+dfsg-3 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.3.12+dfsg-3 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-inst1.4 0.8.16~exp12ubuntu10.16 deb package format runtime library
ii libapt-pkg4.12 0.8.16~exp12ubuntu10.16 package managment runtime library
ii libasn1-8-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - ASN.1 library
ii libattr1 1:2.4.46-5ubuntu1 Extended attribute shared library
ii libbind9-80 1:9.8.1.dfsg.P1-4ubuntu0.8 BIND9 Shared Library used by BIND
ii libblkid1 2.20.1-1ubuntu3 block device id library
ii libboost-iostreams1.46.1 1.46.1-7ubuntu3 Boost.Iostreams Library
ii libbsd0 0.3.0-2 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-1 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.15-0ubuntu10.12 Embedded GNU C Library: Binaries
ii libc-dev-bin 2.15-0ubuntu10.12 Embedded GNU C Library: Development binaries
ii libc6 2.15-0ubuntu10.12 Embedded GNU C Library: Shared libraries
ii libc6-dev 2.15-0ubuntu10.12 Embedded GNU C Library: Development Libraries and Header Files
ii libcap-ng0 0.6.6-1ubuntu1 An alternate POSIX capabilities library
ii libcap2 1:2.22-1ubuntu3 support for getting/setting POSIX.1e capabilities
```

```
ii libclass-accessor-perl 0.34-1 Perl module that automatically generates accessors
ii libclass-isa-perl 0.36-3 report the search path for a class's ISA tree
ii libcomerr2 1.42-1ubuntu2 common error description library
ii libcurl3 7.22.0-3ubuntu4.7 Multi-protocol file transfer library (OpenSSL)
ii libcurl3-gnutls 7.22.0-3ubuntu4.7 Multi-protocol file transfer library (GnuTLS)
ii libcwidget3 0.5.16-3.1ubuntu1 high-level terminal interface library for C++ (runtime files)
ii libdb5.1 5.1.25-11build1 Berkeley v5.1 Database Libraries [runtime]
ii libdbd-mysql-perl 4.020-1build2 Perl5 database interface to the MySQL database
ii libdbi-perl 1.616-1build2 Perl Database Interface (DBI)
ii libdbus-1-3 1.4.18-1ubuntu1.4 simple interprocess messaging system (library)
ii libdbus-glib-1-2 0.98-1ubuntu1.1 simple interprocess messaging system (GLib-based shared library)
ii libdevmapper1.02.1 2:1.02.48-4ubuntu7.4 The Linux Kernel Device Mapper userspace library
ii libdns81 1:9.8.1.dfsg.P1-4ubuntu0.8 DNS Shared Library used by BIND
ii libdrm-intel1 2.4.46-1ubuntu0.0.0.1 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau1a 2.4.46-1ubuntu0.0.0.1 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.46-1ubuntu0.0.0.1 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.46-1ubuntu0.0.0.1 Userspace interface to kernel DRM services -- runtime
ii libedit2 2.11-20080614-3ubuntu2 BSD editline and history libraries
ii libelf1 0.152-1ubuntu3 library to read and write ELF files
ii libept1.4.12 1.0.6~exp1ubuntu1 High-level library for managing Debian package information
ii libevent-2.0-5 2.0.16-stable-1 Asynchronous event notification library
ii libexpat1 2.0.1-7.2ubuntu1.1 XML parsing C library - runtime library
ii libffi6 3.0.11~rc1-5 Foreign Function Interface library runtime
ii libfontconfig1 2.8.0-3ubuntu9.1 generic font configuration library - runtime
ii libfreetype6 2.4.8-1ubuntu2.3 FreeType 2 font engine, shared library files
ii libfribidi0 0.19.2-1 Free Implementation of the Unicode BiDi algorithm
ii libfuse2 2.8.6-2ubuntu2 Filesystem in Userspace (library)
ii libgc1c2 1:7.1-8ubuntu0.12.04.1 conservative garbage collector for C and C++
ii libgcc1 1:4.6.3-1ubuntu5 GCC support library
ii libgcrypt11 1.5.0-3ubuntu0.2 LGPL Crypto library - runtime library
ii libgd2-xpm 2.0.36~rc1~dfsg-6ubuntu2 GD Graphics Library version 2
ii libgdbm3 1.8.3-10 GNU dbm database routines (runtime version)
ii libgeoip1 1.4.8+dfsg-2 non-DNS IP-to-country resolver library
ii libgirepository-1.0-1 1.32.0-1 Library for handling GObject introspection data (runtime library)
ii libglib2.0-0 2.32.4-0ubuntu1 GLib library of C routines
ii libgmp10 2:5.0.2+dfsg-2ubuntu1 Multiprecision arithmetic library
ii libgnutls26 2.12.14-5ubuntu3.5 GNU TLS library - runtime library
ii libgomp1 4.6.3-1ubuntu5 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.10-2ubuntu1 library for common error values and messages in GnuPG components
ii libgpm2 1.20.4-4 General Purpose Mouse - shared library
ii libgssapi-krb5-2 1.10+dfsg~beta1-2ubuntu0.3 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssapi3-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - GSSAPI support library
ii libhcrypto4-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - crypto library
ii libheimbase1-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - Base library
ii libheimntlm0-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - NTLM support library
ii libhtml-template-perl 2.10-1 module for using HTML Templates with Perl
ii libhx509-5-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - X509 support library
ii libidn11 1.23-2 GNU Libidn library, implementation of IETF IDN specifications
ii libio-string-perl 1.08-2 Emulate IO::File interface for in-core strings
ii libisc83 1:9.8.1.dfsg.P1-4ubuntu0.8 ISC Shared Library used by BIND
ii libisccc80 1:9.8.1.dfsg.P1-4ubuntu0.8 Command Channel Library used by BIND
ii libisccfg82 1:9.8.1.dfsg.P1-4ubuntu0.8 Config File Handling Library used by BIND
ii libiw30 30~pre9-5ubuntu2 Wireless tools - library
ii libjpeg-turbo8 1.1.90+svn733-0ubuntu4.4 IJG JPEG compliant runtime library.
ii libjpeg8 8c-2ubuntu7 Independent JPEG Group's JPEG runtime library (dependency package)
ii libjs-jquery 1.7.1-1ubuntu1 JavaScript library for dynamic web applications
ii libk5crypto3 1.10+dfsg~beta1-2ubuntu0.3 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.2-2 Linux Key Management Utilities (library)
ii libklibc 1.5.25-1ubuntu2 minimal libc subset for use with initramfs
ii libkrb5-26-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - libraries
ii libkrb5-3 1.10+dfsg~beta1-2ubuntu0.3 MIT Kerberos runtime libraries
ii libkrb5support0 1.10+dfsg~beta1-2ubuntu0.3 MIT Kerberos runtime libraries - Support library
ii libldap-2.4-2 2.4.28-1.1ubuntu4.4 OpenLDAP libraries
ii liblocale-gettext-perl 1.05-7build1 module using libc functions for internationalization in Perl
ii liblockfile-bin 1.09-3ubuntu0.1 support binaries for and cli utilities based on liblockfile
ii liblockfile1 1.09-3ubuntu0.1 NFS-safe locking library
ii libltdl7 2.4.2-1ubuntu1 A system independent dlopen wrapper for GNU libtool
ii liblwres80 1:9.8.1.dfsg.P1-4ubuntu0.8 Lightweight Resolver Library used by BIND
ii liblzma5 5.1.1alpha+20110809-3 XZ-format compression library
ii libmagic1 5.09-2 File type determination library using "magic" numbers
ii libmcrypt4 2.5.8-3.1 De-/Encryption Library
ii libmount1 2.20.1-1ubuntu3 block device id library
ii libmpc2 0.9-4 multiple precision complex floating-point library
ii libmpfr4 3.1.0-3ubuntu2 multiple precision floating-point computation
ii libmysqlclient18 5.5.46-0ubuntu0.12.04.2 MySQL database client library
ii libncurses5 5.9-4 shared libraries for terminal handling
ii libncursesw5 5.9-4 shared libraries for terminal handling (wide character support)
ii libnet-daemon-perl 0.48-1 Perl module for building portable Perl daemons easily
ii libnewt0.52 0.52.11-2ubuntu10 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.0-1 Netfilter netlink library
ii libnih-dbus1 1.0.3-4ubuntu9.1 NIH D-Bus Bindings Library
ii libnih1 1.0.3-4ubuntu9.1 NIH Utility Library
ii libnl-3-200 3.2.3-2ubuntu2 library for dealing with netlink sockets
ii libnl-genl-3-200 3.2.3-2ubuntu2 library for dealing with netlink sockets - generic netlink
ii libp11-kit0 0.12-2ubuntu1 Library for loading and coordinating access to PKCS#11 modules - runtime
ii libpam-modules 1.1.3-7ubuntu2 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.1.3-7ubuntu2 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.3-7ubuntu2 Runtime support for the PAM library
ii libpam0g 1.1.3-7ubuntu2 Pluggable Authentication Modules library
ii libparse-debianchangelog-perl 1.2.0-1ubuntu1 parse Debian changelogs and output them in other formats
ii libparted0debian1 2.3-8ubuntu5.1 disk partition manipulator - shared library
ii libpcap0.8 1.1.1-10 system interface for user-level packet capture
ii libpci3 1:3.1.8-2ubuntu6 Linux PCI Utilities (shared library)
ii libpciaccess0 0.12.902-1ubuntu0.2 Generic PCI access library for X
ii libpcre3 8.12-4 Perl 5 Compatible Regular Expression Library - runtime files
ii libpcsclite1 1.7.4-2ubuntu2 Middleware to access a smart card using PC/SC (library)
ii libpipeline1 1.2.1-1 pipeline manipulation library
ii libplrpc-perl 0.2020-2 Perl extensions for writing PlRPC servers and clients
ii libplymouth2 0.8.2-2ubuntu31.1 graphical boot animation and logger - shared libraries
```

```
ii libpng12-0 1.2.46-3ubuntu4 PNG library - runtime
ii libpolkit-gobject-1-0 0.104-1ubuntu1.1 PolicyKit Authorization API
ii libpopt0 1.16-3ubuntu1 lib for parsing cmdline parameters
ii libpython2.7 2.7.3-0ubuntu3.4 Shared Python runtime library (version 2.7)
ii libquadmath0 4.6.3-1ubuntu5 GCC Quad-Precision Math Library
ii libreadline6 6.2-8 GNU readline and history libraries, run-time libraries
ii libroken18-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - roken support library
ii librtmp0 2.4~20110711.gitc28f1bab-1 toolkit for RTMP streams (shared library)
ii libsasl2-2 2.1.25.dfsg1-3ubuntu0.1 Cyrus SASL - authentication abstraction library
ii libsasl2-modules 2.1.25.dfsg1-3ubuntu0.1 Cyrus SASL - pluggable authentication modules
ii libselinux1 2.1.0-4.1ubuntu1 SELinux runtime shared libraries
ii libsigc++-2.0-0c2a 2.2.10-0ubuntu2 type-safe Signal Framework for C++ - runtime
ii libslang2 2.2.4-3ubuntu1 S-Lang programming library - runtime version
ii libsqlite3-0 3.7.9-2ubuntu1.1 SQLite 3 shared library
ii libss2 1.42-1ubuntu2 command-line interface parsing library
ii libssl1.0.0 1.0.1-4ubuntu5.11 SSL shared libraries
ii libstdc++6 4.6.3-1ubuntu5 GNU Standard C++ Library v3
ii libsub-name-perl 0.05-1build2 module for assigning a new name to referenced sub
ii libswitch-perl 2.16-2 switch statement for Perl
ii libt1-5 5.1.2-3.4ubuntu1 Type 1 font rasterizer library - runtime
ii libtasn1-3 2.10-1ubuntu1.1 Manage ASN.1 structures (runtime)
ii libterm-readkey-perl 2.30-4build3 A perl module for simple terminal control
ii libtext-charwidth-perl 0.04-7build1 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5 converts between character sets in Perl
ii libtext-wrapi18n-perl 0.06-7 internationalized substitute of Text::Wrap
ii libtimedate-perl 1.2000-1 collection of modules to manipulate date/time information
ii libtinfo5 5.9-4 shared low-level terminfo library for terminal handling
ii libudev0 175-0ubuntu9.4 udev library
ii libusb-0.1-4 2:0.1.12-20 userspace USB programming library
ii libusb-1.0-0 2:1.0.9~rc3-2ubuntu1 userspace USB programming library
ii libuuid1 2.20.1-1ubuntu3 Universally Unique ID library
ii libwind0-heimdal 1.6~git20120311.dfsg.1-2ubuntu0.1 Heimdal Kerberos - stringprep implementation
ii libwrap0 7.6.q-21 Wietse Venema's TCP wrappers library
ii libx11-6 2:1.4.99.1-0ubuntu2.2 X11 client-side library
ii libx11-data 2:1.4.99.1-0ubuntu2.2 X11 client-side library
ii libxapian22 1.2.8-1 Search engine library
ii libxau6 1:1.0.6-4 X11 authorisation library
ii libxcb1 1.8.1-1ubuntu0.2 X C Binding
ii libxdmcp6 1:1.1.0-4 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.0-3ubuntu0.1 X11 miscellaneous extension library
ii libxml2 2.7.8.dfsg-5.1ubuntu4.6 GNOME XML library
ii libxmuu1 2:1.1.0-3 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.9-4 X11 pixmap library
ii linux-firmware 1.79.9 Firmware for Linux kernel drivers
ii linux-generic-lts-saucy 3.11.0.15.14 Generic Linux kernel image and headers
ii linux-headers-3.11.0-15 3.11.0-15.25~precise1 Header files related to Linux kernel version 3.11.0
ii linux-headers-3.11.0-15-generic 3.11.0-15.25~precise1 Linux kernel headers for version 3.11.0 on 32 bit x86 SMP
ii linux-headers-generic-lts-saucy 3.11.0.15.14 Generic Linux kernel headers
ii linux-image-3.11.0-15-generic 3.11.0-15.25~precise1 Linux kernel image for version 3.11.0 on 32 bit x86 SMP
ii linux-image-generic-lts-saucy 3.11.0.15.14 Generic Linux kernel image
ii linux-libc-dev 3.2.0-90.128 Linux Kernel Headers for development
ii locales 2.13+git20120306-3 common files for locale support
ii lockfile-progs 0.1.16 Programs for locking and unlocking files and mailboxes
ii login 1:4.1.4.2+svn3283-3ubuntu5.1 system login tools
ii logrotate 3.7.8-6ubuntu5 Log rotation utility
ii lsb-base 4.0-0ubuntu20.3 Linux Standard Base 4.0 init script functionality
ii lsb-release 4.0-0ubuntu20.3 Linux Standard Base version reporting utility
ii lshw 02.15-2 information about hardware configuration
ii lsof 4.81.dfsg.1-1build1 List open files
ii ltrace 0.5.3-2.1ubuntu2 Tracks runtime library calls in dynamically linked programs
ii makedev 2.3.1-89ubuntu2 creates device files in /dev
ii man-db 2.6.1-2ubuntu1 on-line manual pager
ii manpages 3.35-0.1ubuntu1 Manual pages about using a GNU/Linux system
ii manpages-dev 3.35-0.1ubuntu1 Manual pages about using GNU/Linux for development
ii mawk 1.3.3-17 a pattern scanning and text processing language
ii memtest86+ 4.20-1.1ubuntu1 thorough real-mode memory tester
ii mime-support 3.51-1ubuntu1 MIME files 'mime.types' & 'mailcap', and support programs
ii mlocate 0.23.1-1ubuntu2 quickly find files on the filesystem based on their name
ii module-init-tools 3.16-1ubuntu2 tools for managing Linux kernel modules
ii mount 2.20.1-1ubuntu3 Tools for mounting and manipulating filesystems
ii mountall 2.36.4 filesystem mounting tool
ii mtr-tiny 0.80-1ubuntu1 Full screen ncurses traceroute tool
ii multiarch-support 2.15-0ubuntu10.5 Transitional package to ensure multiarch compatibility
ii mysql-client-5.5 5.5.46-0ubuntu0.12.04.2 MySQL database client binaries
ii mysql-client-core-5.5 5.5.46-0ubuntu0.12.04.2 MySQL database core client binaries
ii mysql-common 5.5.46-0ubuntu0.12.04.2 MySQL database common files, e.g. /etc/mysql/my.cnf
ii mysql-server 5.5.46-0ubuntu0.12.04.2 MySQL database server (metapackage depending on the latest version)
ii mysql-server-5.5 5.5.46-0ubuntu0.12.04.2 MySQL database server binaries and system database setup
ii mysql-server-core-5.5 5.5.46-0ubuntu0.12.04.2 MySQL database server binaries
ii nano 2.2.6-1 small, friendly text editor inspired by Pico
ii ncurses-base 5.9-4 basic terminal type definitions
ii ncurses-bin 5.9-4 terminal-related programs and man pages
ii net-tools 1.60-24.1ubuntu2 The NET-3 networking toolkit
ii netbase 4.47ubuntu1 Basic TCP/IP networking system
ii netcat 1.10-39 TCP/IP swiss army knife -- transitional package
ii netcat-openbsd 1.89-4ubuntu1 TCP/IP swiss army knife
ii netcat-traditional 1.10-39 TCP/IP swiss army knife
ii ntfs-3g 1:2012.1.15AR.1-1ubuntu1.2 read/write NTFS driver for FUSE
ii ntpdate 1:4.2.6.p3+dfsg-1ubuntu3.1 client for setting system time from NTP servers
ii openssh-client 1:5.9p1-5ubuntu1.1 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:5.9p1-5ubuntu1.1 secure shell (SSH) server, for secure access from remote machines
ii openssl 1.0.1-4ubuntu5.11 Secure Socket Layer (SSL) binary and related cryptographic tools
ii os-prober 1.51ubuntu3 utility to detect other OSes on a set of drives
ii parted 2.3-8ubuntu5.1 disk partition manipulator
ii passwd 1:4.1.4.2+svn3283-3ubuntu5.1 change and administer password and group data
ii patch 2.6.1-3 Apply a diff file to an original
ii pciutils 1:3.1.8-2ubuntu6 Linux PCI Utilities
ii perl 5.14.2-6ubuntu2.3 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.14.2-6ubuntu2.3 minimal Perl system
```

```
ii perl-modules 5.14.2-6ubuntu2.3 Core Perl modules
ii php5 5.3.10-1ubuntu3.19 server-side, HTML-embedded scripting language (metapackage)
ii php5-cli 5.3.10-1ubuntu3.21 command-line interpreter for the php5 scripting language
ii php5-common 5.3.10-1ubuntu3.21 Common files for packages built from the php5 source
ii php5-gd 5.3.10-1ubuntu3.21 GD module for php5
ii php5-mcrypt 5.3.5-0ubuntu1 MCrypt module for php5
ii php5-mysql 5.3.10-1ubuntu3.21 MySQL module for php5
ii plymouth 0.8.2-2ubuntu31.1 graphical boot animation and logger - main package
ii plymouth-theme-ubuntu-text 0.8.2-2ubuntu31.1 graphical boot animation and logger - ubuntu-logo theme
ii popularity-contest 1.53ubuntu1 Vote for your favourite packages automatically
ii powermgmt-base 1.31 Common utils and configs for power management
ii ppp 2.4.5-5ubuntu1 Point-to-Point Protocol (PPP) - daemon
ii pppconfig 2.3.18+nmu3ubuntu1 A text menu based utility for configuring ppp
ii pppoeconf 1.20ubuntu1 configures PPPoE/ADSL connections
ii procps 1:3.2.8-11ubuntu6.3 /proc file system utilities
ii psmisc 22.15-2ubuntu1.1 utilities that use the proc file system
ii python 2.7.3-0ubuntu2.2 interactive high-level object-oriented language (default version)
ii python-apport 2.0.1-0ubuntu17.6 apport crash report handling library
ii python-apt 0.8.3ubuntu7.2 Python interface to libapt-pkg
ii python-apt-common 0.8.3ubuntu7.2 Python interface to libapt-pkg (locales)
ii python-chardet 2.0.1-2build1 universal character encoding detector
ii python-crypto 2.4.1-1ubuntu0.1 cryptographic algorithms and protocols for Python
ii python-dbus 1.0.0-1ubuntu1 simple interprocess messaging system (Python interface)
ii python-dbus-dev 1.0.0-1ubuntu1 main loop integration development files for python-dbus
ii python-debian 0.1.21ubuntu1 Python modules to work with Debian-related data formats
ii python-gdbm 2.7.3-1ubuntu1 GNU dbm database support for Python
ii python-gi 3.2.2-1~precise Python 2.x bindings for gobject-introspection libraries
ii python-gnupginterface 0.3.2-9.1ubuntu3 Python interface to GnuPG (GPG)
ii python-httplib2 0.7.2-1ubuntu2.1 comprehensive HTTP client library written for Python
ii python-keyring 0.9.2-0ubuntu0.12.04.2 store and access your passwords safely
ii python-launchpadlib 1.9.12-1 Launchpad web services client library
ii python-lazr.restfulclient 0.12.0-1ubuntu1.1 client for lazr.restful-based web services
ii python-lazr.uri 1.0.3-1 library for parsing, manipulating, and generating URIs
ii python-minimal 2.7.3-0ubuntu2.2 minimal subset of the Python language (default version)
ii python-newt 0.52.11-2ubuntu10 A NEWT module for Python
ii python-oauth 1.0.1-3build1 Python library implementing of the OAuth protocol
ii python-openssl 0.12-1ubuntu2.1 Python wrapper around the OpenSSL library
ii python-pam 0.4.2-12.2ubuntu4 A Python interface to the PAM library
ii python-pkg-resources 0.6.24-1ubuntu1 Package Discovery and Resource Access using pkg_resources
ii python-problem-report 2.0.1-0ubuntu17.6 Python library to handle problem reports
ii python-serial 2.5-2.1build1 pyserial - module encapsulating access for the serial port
ii python-simplejson 2.3.2-1 simple, fast, extensible JSON encoder/decoder for Python
ii python-twisted-bin 11.1.0-1ubuntu2 Event-based framework for internet applications
ii python-twisted-core 11.1.0-1ubuntu2 Event-based framework for internet applications
ii python-wadllib 1.3.0-2 Python library for navigating WADL files
ii python-xapian 1.2.8-1 Xapian search engine interface for Python
ii python-zope.interface 3.6.1-1ubuntu3 Interfaces for Python
ii python2.7 2.7.3-0ubuntu3.4 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.3-0ubuntu3.4 Minimal subset of the Python language (version 2.7)
ii readline-common 6.2-8 GNU readline and history libraries, common files
ii resolvconf 1.63ubuntu16 name server information handler
ii rsync 3.0.9-1ubuntu1 fast, versatile, remote (and local) file-copying tool
ii rsyslog 5.8.6-1ubuntu8.6 reliable system and kernel logging daemon
ii screen 4.0.3-14ubuntu8 terminal multiplexor with VT100/ANSI terminal emulation
ii sed 4.2.1-9 The GNU sed stream editor
ii sensible-utils 0.0.6ubuntu2 Utilities for sensible alternative selection
ii sgml-base 1.26+nmu1ubuntu1 SGML infrastructure and SGML catalog file support
ii squid 3.1.19-1ubuntu3.12.04.3 dummy transitional package from squid to squid3
ii squid-langpack 20111114-1 Localized error pages for Squid
ii squid3 3.1.19-1ubuntu3.12.04.3 Full featured Web Proxy cache (HTTP proxy)
ii squid3-common 3.1.19-1ubuntu3.12.04.3 Full featured Web Proxy cache (HTTP proxy) - common files
ii ssh-import-id 2.10-0ubuntu1 securely retrieve an SSH public key and install it locally
ii ssl-cert 1.0.28ubuntu0.1 simple debconf wrapper for OpenSSL
ii strace 4.5.20-2.3ubuntu1 A system call tracer
ii sudo 1.8.3p1-1ubuntu3.4 Provide limited super user privileges to specific users
ii sysv-rc 2.88dsf-13.10ubuntu11.1 System-V-like runlevel change mechanism
ii sysvinit-utils 2.88dsf-13.10ubuntu11.1 System-V-like utilities
ii tar 1.26-4ubuntu1 GNU version of the tar archiving utility
ii tasksel 2.88ubuntu9 Tool for selecting tasks for installation on Debian systems
ii tasksel-data 2.88ubuntu9 Official tasks used for installation of Debian systems
ii tcpd 7.6.q-21 Wietse Venema's TCP wrapper utilities
ii tcpdump 4.2.1-1ubuntu2 command-line network traffic analyzer
ii telnet 0.17-36build1 The telnet client
ii time 1.7-23.1 The GNU time program for measuring cpu resource usage
ii tmux 1.6-1ubuntu1 terminal multiplexer
ii ttf-dejavu-core 2.33-2ubuntu1 Vera font family derivate with additional characters
ii tzdata 2013g-0ubuntu0.12.04 time zone and daylight-saving time data
ii ubuntu-keyring 2011.11.21.1 GnuPG keys of the Ubuntu archive
ii ubuntu-minimal 1.267.1 Minimal core of Ubuntu
ii ubuntu-standard 1.267.1 The Ubuntu standard system
ii ucf 3.0025+nmu2ubuntu1 Update Configuration File: preserve user changes to config files.
ii udev 175-0ubuntu9.4 rule-based device node and kernel event manager
ii ufw 0.31.1-1 program for managing a Netfilter firewall
ii unzip 6.0-4ubuntu2.5 De-archiver for .zip files
ii update-manager-core 1:0.156.14.11 manage release upgrades
ii update-notifier-common 0.119ubuntu8.6 Files shared between update-notifier and other packages
ii upstart 1.5-0ubuntu7.2 event-based init daemon
ii ureadahead 0.100.0-12 Read required files in advance
ii usbutils 1:005-1 Linux USB utilities
ii util-linux 2.20.1-1ubuntu3 Miscellaneous system utilities
ii uuid-runtime 2.20.1-1ubuntu3 runtime components for the Universally Unique ID library
ii vim 2:7.3.429-2ubuntu2.1 Vi IMproved - enhanced vi editor
ii vim-common 2:7.3.429-2ubuntu2.1 Vi IMproved - Common files
ii vim-runtime 2:7.3.429-2ubuntu2.1 Vi IMproved - Runtime files
ii vim-tiny 2:7.3.429-2ubuntu2.1 Vi IMproved - enhanced vi editor - compact version
ii w3m 0.5.3-5ubuntu1.1 WWW browsable pager with excellent tables/frames support
ii wget 1.13.4-2ubuntu1 retrieves files from the web
ii whiptail 0.52.11-2ubuntu10 Displays user-friendly dialog boxes from shell scripts
ii whoopsie 0.1.33 Ubuntu crash database submission daemon
```

```
ii wireless-tools 30~pre9-5ubuntu2 Tools for manipulating Linux Wireless Extensions
ii wpasupplicant 0.7.3-6ubuntu2.2 client support for WPA and WPA2 (IEEE 802.11i)
ii xauth 1:1.0.6-1 X authentication utility
ii xkb-data 2.5-1ubuntu1.3 X Keyboard Extension (XKB) configuration data
ii xml-core 0.13 XML infrastructure and XML catalog file support
ii xz-lzma 5.1.1alpha+20110809-3 XZ-format compression utilities - compatibility commands
ii xz-utils 5.1.1alpha+20110809-3 XZ-format compression utilities
ii zlib1g 1:1.2.3.4.dfsg-3ubuntu4 compression library - runtime
```

49692 - Squid Proxy Version Detection -

Synopsis

It was possible to obtain the version number of the remote Squid proxy server.

Description

The remote host is running the Squid proxy server, an open source proxy server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/09/28, Modified: 2024/06/17

Plugin Output

tcp/3128/http_proxy

```
URL : http://10.136.108.108:3128/
Version : 3.1.19
Source : Server: squid/3.1.19
```

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: 'sickos'
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: 'sickos'
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 3.11.0-15-generi Thu Nov 13 20:57 - 22:57 (02:00)
reboot system boot 3.11.0-15-generi Sun Dec 6 21:10 - 21:18 (00:07)
reboot system boot 3.11.0-15-generi Sun Dec 6 07:15 - 07:28 (00:12)
reboot system boot 3.11.0-15-generi Sun Dec 6 06:23 - 07:15 (00:51)
reboot system boot 3.11.0-15-generi Sun Dec 6 06:22 - 06:23 (00:00)
reboot system boot 3.11.0-15-generi Sun Dec 6 05:56 - 06:21 (00:25)
reboot system boot 3.11.0-15-generi Sat Dec 5 17:41 - 06:21 (12:39)
reboot system boot 3.11.0-15-generi Sat Dec 5 08:03 - 06:21 (22:18)
reboot system boot 3.11.0-15-generi Fri Sep 25 09:34 - 08:02 (70+22:27)
reboot system boot 3.11.0-15-generi Tue Sep 22 09:25 - 09:33 (3+00:08)
reboot system boot 3.11.0-15-generi Tue Sep 22 08:19 - 09:24 (01:04)

wtmp begins Tue Sep 22 08:19:56 2015
```

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 10.136.108.33 to 10.136.108.108 :
10.136.108.33
10.136.108.108

Hop Count: 1
```

192709 - Tukaani XZ Utils Installed (Linux / Unix) -

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:
- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

Path : /usr/bin/xz
Version : 5.1.1
Associated Package : xz-utils 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package

Path : /usr/lib/i386-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
```

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 0.1 3532 1920 ? Ss 20:57 0:00 /sbin/init
root 2 0.0 0.0 0 0 ? S 20:57 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 20:57 0:01 [ksoftirqd/0]
root 4 0.0 0.0 0 0 ? S 20:57 0:00 [kworker/0:0]
root 5 0.0 0.0 0 0 ? S< 20:57 0:00 [kworker/0:0H]
root 7 0.0 0.0 0 0 ? S 20:57 0:00 [migration/0]
root 8 0.0 0.0 0 0 ? S 20:57 0:00 [rcu_bh]
root 9 0.0 0.0 0 0 ? S 20:57 0:01 [rcu_sched]
root 10 0.0 0.0 0 0 ? S 20:57 0:00 [watchdog/0]
root 11 0.0 0.0 0 0 ? S< 20:57 0:00 [khelper]
root 12 0.0 0.0 0 0 ? S 20:57 0:00 [kdevtmpfs]
root 13 0.0 0.0 0 0 ? S< 20:57 0:00 [netns]
root 14 0.0 0.0 0 0 ? S< 20:57 0:00 [writeback]
root 15 0.0 0.0 0 0 ? S< 20:57 0:00 [kintegrityd]
root 16 0.0 0.0 0 0 ? S< 20:57 0:00 [bioset]
root 17 0.0 0.0 0 0 ? S< 20:57 0:00 [kworker/u3:0]
root 18 0.0 0.0 0 0 ? S< 20:57 0:00 [kblockd]
root 19 0.0 0.0 0 0 ? S< 20:57 0:00 [ata_sff]
root 20 0.0 0.0 0 0 ? S 20:57 0:00 [khubd]
root 21 0.0 0.0 0 0 ? S< 20:57 0:00 [md]
root 22 0.0 0.0 0 0 ? S< 20:57 0:00 [devfreq_wq]
root 23 0.0 0.0 0 0 ? S 20:57 0:03 [kworker/0:1]
root 25 0.0 0.0 0 0 ? S 20:57 0:00 [khungtaskd]
root 26 0.0 0.0 0 0 ? S 20:57 0:00 [kswapd0]
root 27 0.0 0.0 0 0 ? SN 20:57 0:00 [ksmd]
root 28 0.0 0.0 0 0 ? SN 20:57 0:00 [khugepaged]
root 29 0.0 0.0 0 0 ? S 20:57 0:00 [fsnotify_mark]
root 30 0.0 0.0 0 0 ? S 20:57 0:00 [ecryptfs-kthrea]
root 31 0.0 0.0 0 0 ? S< 20:57 0:00 [crypto]
root 43 0.0 0.0 0 0 ? S< 20:57 0:00 [kthrotld]
root 46 0.0 0.0 0 0 ? S< 20:57 0:00 [dm_bufio_cache]
root 66 0.0 0.0 0 0 ? S< 20:57 0:00 [deferwq]
root 67 0.0 0.0 0 0 ? S< 20:57 0:00 [charger_manager]
root 217 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_0]
root 218 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_1]
root 219 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_2]
root 220 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_3]
root 221 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_4]
root 222 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_5]
root 223 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_6]
root 224 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_7]
root 225 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_8]
root 226 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_9]
root 227 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_10]
root 228 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_11]
root 229 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_12]
root 230 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_13]
root 231 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_14]
root 232 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_15]
root 233 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_16]
root 234 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_17]
root 235 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_18]
root 236 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_19]
root 237 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_20]
root 238 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_21]
root 239 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_22]
root 240 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_23]
root 241 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_24]
root 242 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_25]
root 243 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_26]
root 244 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_27]
root 245 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_28]
root 246 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_29]
root 248 0.0 0.0 0 0 ? S< 20:57 0:00 [mpt_poll_0]
root 249 0.0 0.0 0 0 ? S< 20:57 0:00 [mpt/0]
root 275 0.0 0.0 0 0 ? S 20:57 0:00 [kworker/u2:29]
root 278 0.0 0.0 0 0 ? S 20:57 0:00 [scsi_eh_30]
root 356 0.0 0.0 0 0 ? S 20:57 0:00 [jbd2/sda1-8]
root 357 0.0 0.0 0 0 ? S< 20:57 0:00 [ext4-rsv-conver]
root 358 0.0 0.0 0 0 ? S< 20:57 0:00 [ext4-unrsv-conv]
root 454 0.0 0.0 2832 608 ? S 20:57 0:00 upstart-udev-bridge --daemon
root 456 0.0 0.1 3104 1308 ? Ss 20:57 0:00 /sbin/udevd --daemon
root 629 0.0 0.0 3100 824 ? S 20:57 0:00 /sbin/udevd --daemon
root 630 0.0 0.0 3100 824 ? S 20:57 0:00 /sbin/udevd --daemon
root 785 0.0 0.0 0 0 ? S< 20:57 0:00 [kpsmoused]
root 821 0.0 0.0 2844 348 ? S 20:57 0:00 upstart-socket-bridge --daemon
102 924 0.0 0.0 3256 892 ? Ss 20:57 0:00 dbus-daemon --system --fork --activation=upstart
syslog 927 0.0 0.1 30164 1336 ? Sl 20:57 0:00 rsyslogd -c5
root 961 0.0 0.0 2924 848 ? Ss 20:57 0:00 dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf
/var/lib/dhcp/dhclient.eth0.leases -1 eth0
root 983 0.0 0.2 6680 2412 ? Ss 20:57 0:00 /usr/sbin/sshd -D
root 1066 0.0 0.0 4628 856 tty4 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty4
root 1074 0.0 0.0 4628 848 tty5 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty5
root 1082 0.0 0.0 4628 852 tty2 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty2
root 1083 0.0 0.0 4628 848 tty3 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty3
root 1087 0.0 0.0 4628 852 tty6 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty6
root 1105 0.0 0.0 2172 620 ? Ss 20:57 0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
root 1108 0.0 0.0 2616 932 ? Ss 20:57 0:00 cron
daemon 1109 0.0 0.0 2468 348 ? Ss 20:57 0:00 atd
proxy 1115 0.3 1.6 41388 16432 ? Ss 20:57 0:22 /usr/sbin/squid3 -N -YC -f /etc/squid3/squid.conf
```

```
whoopsie 1142 0.0 0.3 24440 3140 ? Ssl 20:57 0:00 whoopsie
mysql 1163 0.0 3.3 326148 34164 ? Ssl 20:57 0:03 /usr/sbin/mysqld
proxy 1174 0.0 0.0 3220 608 ? Ss 20:57 0:00 (unlinkd)
root 1176 0.0 0.7 37900 7656 ? Ss 20:57 0:01 /usr/sbin/apache2 -k start
root 1203 0.0 0.0 0 0 ? S< 20:57 0:00 [kworker/u3:1]
www-data 1213 0.0 0.8 39784 9224 ? S 20:57 0:00 /usr/sbin/apache2 -k start
www-data 1214 0.0 0.8 39500 8988 ? S 20:57 0:00 /usr/sbin/apache2 -k start
www-data 1215 0.0 0.9 39756 9316 ? S 20:57 0:00 /usr/sbin/apache2 -k start
www-data 1216 0.0 0.9 40036 9504 ? S 20:57 0:00 /usr/sbin/apache2 -k start
www-data 1221 0.0 0.9 40580 9596 ? S 20:57 0:00 /usr/sbin/apache2 -k start
root 1236 0.0 0.0 4628 852 tty1 Ss+ 20:57 0:00 /sbin/getty -8 38400 tty1
root 1385 0.0 0.0 0 0 ? S 21:02 0:01 [kworker/u2:0]
www-data 1499 0.0 0.8 39496 8284 ? S 21:36 0:00 /usr/sbin/apache2 -k start
www-data 1522 0.0 0.9 39776 9396 ? S 21:40 0:00 /usr/sbin/apache2 -k start
www-data 1532 0.0 0.9 40276 9404 ? S 21:43 0:00 /usr/sbin/apache2 -k start
www-data 1533 0.0 0.4 37964 4764 ? S 21:43 0:00 /usr/sbin/apache2 -k start
www-data 1534 0.0 0.6 38504 6352 ? S 21:43 0:00 /usr/sbin/apache2 -k start
www-data 1698 0.0 0.0 2232 540 ? S 22:11 0:00 sh -c uname -a; w; id; /bin/sh -i
www-data 1702 0.0 0.0 2232 540 ? S 22:11 0:00 /bin/sh -i
www-data 1713 0.0 0.4 9108 4288 ? S 22:14 0:00 python -c import pty; pty.spawn("/bin/sh")
www-data 1714 0.0 0.0 2232 568 pts/0 Ss+ 22:14 0:00 /bin/sh
root 8542 2.0 0.2 9644 3020 ? Ss 22:58 0:00 sshd: sickos [priv]
root 8960 2.0 0.2 9504 2960 ? Ss 22:58 0:00 sshd: sickos [priv]
root 9114 0.0 0.0 2232 540 ? S 22:58 0:00 sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
run-parts --lsbsysinit /etc/update-motd.d > /var/run/motd.new
root 9116 0.0 0.0 2140 544 ? S 22:58 0:00 run-parts --lsbsysinit /etc/update-motd.d
root 9146 0.0 0.0 2232 580 ? S 22:58 0:00 /bin/sh -e /usr/lib/update-notifier/update-motd-updates-available
root 9153 0.0 0.2 8024 2416 ? Ss 22:58 0:00 sshd: [accepted]
sshd 9163 0.0 0.0 8024 896 ? S 22:58 0:00 sshd: [net]
sickos 9182 0.0 0.1 9644 1660 ? S 22:58 0:00 sshd: sickos@notty
sickos 9185 0.0 0.1 5172 1120 ? Ss 22:58 0:00 bash -c /bin/ps auxww 2>/dev/null
sickos 9186 0.0 0.1 4936 1144 ? R 22:58 0:00 /bin/ps auxww
```

152742 - Unix Software Discovery Commands Available -

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Unix software discovery checks are available.

Account : sickos
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

```
Nessus detected 2 installs of Vim:

Path : /usr/bin/vim.tiny
Version : 7.3

Path : /usr/bin/vim.basic
Version : 7.3
```

182848 - libcurl Installed (Linux / Unix) -

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

Path : /usr/lib/i386-linux-gnu/libcurl.so.4.2.0
Version : 7.22.0
Associated Package : libcurl3 7.22.0-3ubuntu4.7
Managed by OS : True

Path : /usr/lib/i386-linux-gnu/libcurl-gnutls.so.4.2.0
Version : 7.22.0
Associated Package : libcurl3-gnutls 7.22.0-3ubuntu4.7
Managed by OS : True
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 94% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2287-1): Update the affected linux-image-3.11-generic and / or linux-image-3.11-generic-lpae packages.	53	1
MySQL Denial of Service (Jul 2020 CPU): Refer to the vendor advisory.	27	1
Ubuntu 12.04 LTS : eglibc vulnerability (USN-3323-2) (Stack Clash): Update the affected libc6 package. Note that the updated package may not be immediately available from the package repository or its mirrors.	9	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1): Update the affected file and / or libmagic1 packages.	3	1
Ubuntu 12.04 LTS : openssl vulnerability (USN-2863-1) (SLOTH): Update the affected libssl1.0.0 package.	3	1
Ubuntu 12.04 LTS : pam regression (USN-2935-3): Update the affected libpam-modules package.	3	1
Ubuntu 12.04 LTS : rtmpdump vulnerabilities (USN-3283-2): Update the affected librtmp0 package. Note that the updated packages may not be immediately available from the package repository and its mirrors.	3	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1): Update the affected libcurl3, libcurl3-gnutls and / or libcurl3-nss packages.	2	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1): Update the affected libgnutls26 package.	2	1
Ubuntu 12.04 LTS : FreeType vulnerabilities (USN-3282-2): Update the affected libfreetype6 package.	2	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2155-1): Update the affected openssh-server package.	1	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3 vulnerability (USN-2125-1): Update the affected packages.	1	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : perl vulnerability (USN-2099-1): Update the affected perl-modules package.	1	1
Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1): Update the affected gnupg package.	1	1
Ubuntu 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2164-1): Update the affected openssh-client package.	1	1
Ubuntu 12.04 LTS : libnl3 vulnerability (USN-3311-2): Update the affected libnl-3-200 package. Note that the updated package may not be immediately available from the package repository and its mirrors.	1	1
Ubuntu 12.04 LTS : python-crypto vulnerability (USN-3199-3): Update the affected python-crypto and / or python3-crypto packages.	1	1
Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1): Update the affected sudo and / or sudo-ldap packages.	0	1