Tenable.io Report

Tenable.io Report

Tue, 04 May 2021 14:10:12 UTC

Table Of Contents

Vulnerabilities By Host

172.16.4.38

Scan Information

Start time:	2021/05/02 17:01
End time:	2021/05/03 07:51

Host Information

OS:	[0: Linux Kernel 4.12.14-8.58-azure on SuSE15.1]

Results Summary

Critical	High	Medium	Low	Info	Total
0	8	16	3	42	69

Results Details

/

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.

See Also

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
The following IPv4 addresses are set on the remote host :

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

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.2

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.2 (E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2015-4000
BID	74733

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2015/05/28, Modification date: 2021/02/03

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

146553 - SUSE SLED15 / SLES15 Security Update : jasper (SUSE-SU-2021:0488-1)

Synopsis

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

Description

This update for jasper fixes the following issues :
bsc#1179748 CVE-2020-27828: Fix heap overflow by checking maxrlvls
bsc#1181483 CVE-2021-3272: Fix buffer over-read in jp2_decode

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

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1179748

https://bugzilla.suse.com/show_bug.cgi?id=1181483

https://www.suse.com/security/cve/CVE-2020-27828/

https://www.suse.com/security/cve/CVE-2021-3272/

http://www.nessus.org/u?befb2bd2

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-488=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-488=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-488=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-488=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-488=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-488=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-488=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-488=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP3-2021-488=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP2-2021-488=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-488=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-488=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-488=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-488=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-488=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-488=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-488=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-3272
CVE	CVE-2020-27828

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/02/17, Modification date: 2021/02/19

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libjasper4-2.0.14-3.16.1
Should be                : libjasper4-2.0.14-3.19.1
```

148868 - SUSE SLED15 / SLES15 Security Update : sudo (SUSE-SU-2021:1275-1)

Synopsis

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

Description

This update for sudo fixes the following issues :
L3: Tenable Scan reports sudo is vulnerable to CVE-2021-3156 (bsc#1183936)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://www.suse.com/security/cve/CVE-2021-3156/

https://bugzilla.suse.com/show_bug.cgi?id=1183936

http://www.nessus.org/u?5634479f

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE MicroOS 5.0 :
zypper in -t patch SUSE-SUSE-MicroOS-5.0-2021-1275=1
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-1275=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-1275=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-1275=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-1275=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-1275=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-1275=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-1275=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-1275=1

SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-1275=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-1275=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-1275=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1275=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1275=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-1275=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

9.8

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (E:H/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.3 (E:H/RL:OF/RC:C)

References

CVE CVE-2021-3156

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/04/21, Modification date: 2021/04/23

Ports

172.16.4.38 (TCP/0) Vulnerability State: New

```
Remote package installed : sudo-1.8.22-4.15.1
Should be                : sudo-1.8.22-4.18.1
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2019/01/08, Modification date: 2020/08/07

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/10/12, Modification date: 2018/06/19

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
reboot   system boot  4.12.14-8.58-azu Mon May  3 08:46   still running
reboot   system boot  4.12.14-8.58-azu Sun May  2 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Sat May  1 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Fri Apr 30 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Thu Apr 29 08:46 - 21:20  (12:33)
reboot   system boot  4.12.14-8.58-azu Wed Apr 28 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Tue Apr 27 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Mon Apr 26 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Sun Apr 25 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Sat Apr 24 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Fri Apr 23 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Thu Apr 22 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Wed Apr 21 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Wed Apr 21 02:55 - 03:01  (00:06)
reboot   system boot  4.12.14-8.58-azu Wed Apr 21 02:11 - 02:54  (00:43)
reboot   system boot  4.12.14-8.58-azu Tue Apr 20 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Mon Apr 19 08:46 - 21:21  (12:35)
reboot   system boot  4.12.14-8.58-azu Sun Apr 18 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Sat Apr 17 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Fri Apr 16 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.58-azu Thu Apr 15 23:30 - 23:37  (00:07)
reboot   system boot  4.12.14-8.38-azu Thu Apr 15 23:14 - 23:29  (00:15)
reboot   system boot  4.12.14-8.38-azu Thu Apr 15 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.38-azu Wed Apr 14 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.38-azu Tue Apr 13 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.38-azu Mon Apr 12 08:46 - 21:20  (12:34)
reboot   system boot  4.12.14-8.38-azu Sun Apr 11 08:45 - 21:20  (12:34)
reboot   system [...]
```

146367 - SUSE SLED15 / SLES15 Security Update : python (SUSE-SU-2021:0355-1)

Synopsis

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

Description

This update for python fixes the following issues :
buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution (bsc#1181126, CVE-2021-3177).
Provide the newest setuptools wheel (bsc#1176262, CVE-2019-20916) in their correct form (bsc#1180686).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1176262

https://bugzilla.suse.com/show_bug.cgi?id=1180686

https://bugzilla.suse.com/show_bug.cgi?id=1181126

https://www.suse.com/security/cve/CVE-2019-20916/

https://www.suse.com/security/cve/CVE-2021-3177/

http://www.nessus.org/u?d3fea06e

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-355=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-355=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-355=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-355=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-355=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-355=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-355=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-355=1
SUSE Linux Enterprise Module for Python2 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Python2-15-SP3-2021-355=1
SUSE Linux Enterprise Module for Python2 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Python2-15-SP2-2021-355=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP3-2021-355=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP2-2021-355=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-355=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-355=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-355=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-355=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-355=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-355=1

SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-355=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

7.4

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-3177
CVE	CVE-2019-20916

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/02/10, Modification date: 2021/02/12

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libpython2_7-1_0-2.7.17-7.47.1
Should be                : libpython2_7-1_0-2.7.17-7.52.2

Remote package installed : python-2.7.17-7.47.1
Should be                : python-2.7.17-7.52.2

Remote package installed : python-base-2.7.17-7.47.1
Should be                : python-base-2.7.17-7.52.2

Remote package installed : python-xml-2.7.17-7.47.1
Should be                : python-xml-2.7.17-7.52.2
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote host.

See Also

Solution

None

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/12/19, Modification date: 2019/04/04

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
----------[ User Accounts ]----------

User         : iplroot
Home folder  : /home/iplroot
Start script : /bin/bash
Groups       : users

User         : sccadmin
Home folder  : /opt/sap/scc
Start script : /bin/false
Groups       : sccgroup

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

User         : omsagent
Home folder  : /var/opt/microsoft/omsagent/run
Start script : /bin/bash
Groups       : omiusers

User         : nxautomation
Home folder  : /home/nxautomation/run
Start script : /bin/bash
Groups       : omsagent
               omiusers
               nxautomation

User         : systemd-network
Home folder  : /
Start script : /sbin/nologin
Groups       : systemd-network

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

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

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

User         : nobody
Home folder  : /var/lib/nobody
Start script : /bin/bash
Groups       : nogroup
               nobody

User         : man
Home folder  : /var/lib/empty
Start script : /sbin/nologin
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : /sbin/nologin
Groups       : lp

User         : systemd-coredump
Home folder  : /
Start script : /sbin/nologin
Groups       : systemd-coredump
```

```
User         : systemd-timesync
Home folder  : /
Start script : /sbin/nologin
Groups       : systemd-timesync

User         : rpc
Home folder  : /var/lib/empty
Start script : /sbin/nologin
Groups       : nobody

User         : nscd
Home folder  : /run/nscd
Start script : /sbin/nologin
Groups       : nscd

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

User         : polkitd
Home folder  : /var/lib/polkit
Start script : /sbin/nologin
Groups       : polkitd

User         : at
Home folder  : /var/spool/atjobs
Start script : /bin/bash
Groups       : at

User         : statd
Home folder  : [...]
```

148504 - SUSE SLES15 Security Update : open-iscsi (SUSE-SU-2021:1164-1)

Synopsis

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

Description

This update for open-iscsi fixes the following issues :
CVE-2020-17437: uIP Out-of-Bounds Write (bsc#1179908)
CVE-2020-17438: uIP Out-of-Bounds Write (bsc#1179908)
CVE-2020-13987: uIP Out-of-Bounds Read (bsc#1179908)
CVE-2020-13988: uIP Integer Overflow (bsc#1179908)
Enabled no-wait ('-W') iscsiadm option for iscsi login service (bsc#1173886, bsc#1183421)
Added the ability to perform async logins (bsc#1173886)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1179908

https://www.suse.com/security/cve/CVE-2020-13987/

https://www.suse.com/security/cve/CVE-2020-13988/

https://www.suse.com/security/cve/CVE-2020-17437/

https://www.suse.com/security/cve/CVE-2020-17438/

https://bugzilla.suse.com/show_bug.cgi?id=1173886

https://bugzilla.suse.com/show_bug.cgi?id=1183421

http://www.nessus.org/u?a8459214

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-1164=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-1164=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-1164=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-1164=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-1164=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-1164=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-1164=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-1164=1
SUSE Linux Enterprise Module for Legacy Software 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Legacy-15-SP3-2021-1164=1
SUSE Linux Enterprise Module for Legacy Software 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Legacy-15-SP2-2021-1164=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-1164=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-1164=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1164=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1164=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-1164=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2020-17437
CVE	CVE-2020-17438
CVE	CVE-2020-13987
CVE	CVE-2020-13988

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/04/14, Modification date: 2021/04/16

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : iscsiuio-0.7.8.2-13.37.1
Should be                : iscsiuio-0.7.8.2-13.42.1

Remote package installed : libopeniscsiusr0_2_0-2.0.876-13.37.1
Should be                : libopeniscsiusr0_2_0-2.0.876-13.42.1

Remote package installed : open-iscsi-2.0.876-13.37.1
Should be                : open-iscsi-2.0.876-13.42.1
```

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.

See Also

Solution

Disable any unused interfaces.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/06/30, Modification date: 2018/08/13

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

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

  - 00:0d:3a:3e:46:d8 (interfaces eth0 & eth1)
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

See Also

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

Vulnerability Priority Rating (VPR)

0.8

CVSS v3.0 Base Score

0.0 (AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS Base Score

0.0 (AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/08/01, Modification date: 2019/10/04

Ports

172.16.4.38 (ICMP/0) Vulnerability State: Active

```
The remote clock is synchronized with the local clock.
```

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/04/26, Modification date: 2017/08/28

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

146978 - SUSE SLES15 Security Update : grub2 (SUSE-SU-2021:0684-1)

Synopsis

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

Description

This update for grub2 fixes the following issues :
grub2 now implements the new 'SBAT' method for SHIM based secure boot revocation. (bsc#1182057)
Following security issues are fixed that can violate secure boot constraints :
CVE-2020-25632: Fixed a use-after-free in rmmod command (bsc#1176711)
CVE-2020-25647: Fixed an out-of-bound write in grub_usb_device_initialize() (bsc#1177883)
CVE-2020-27749: Fixed a stack-based buffer overflow in grub_parser_split_cmdline (bsc#1179264)
CVE-2020-27779, CVE-2020-14372: Disallow cutmem and acpi commands in secure boot mode (bsc#1179265 bsc#1175970)
CVE-2021-20225: Fixed a heap out-of-bounds write in short form option parser (bsc#1182262)
CVE-2021-20233: Fixed a heap out-of-bound write due to mis-calculation of space required for quoting (bsc#1182263)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1175970

https://bugzilla.suse.com/show_bug.cgi?id=1176711

https://bugzilla.suse.com/show_bug.cgi?id=1177883

https://bugzilla.suse.com/show_bug.cgi?id=1179264

https://bugzilla.suse.com/show_bug.cgi?id=1179265

https://bugzilla.suse.com/show_bug.cgi?id=1182057

https://bugzilla.suse.com/show_bug.cgi?id=1182262

https://bugzilla.suse.com/show_bug.cgi?id=1182263

https://www.suse.com/security/cve/CVE-2020-14372/

https://www.suse.com/security/cve/CVE-2020-25632/

https://www.suse.com/security/cve/CVE-2020-25647/

https://www.suse.com/security/cve/CVE-2020-27749/

https://www.suse.com/security/cve/CVE-2020-27779/

https://www.suse.com/security/cve/CVE-2021-20225/

https://www.suse.com/security/cve/CVE-2021-20233/

http://www.nessus.org/u?85a28919

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-684=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-684=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-684=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-684=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-684=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-684=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-684=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-684=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-684=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

7.3

CVSS v3.0 Base Score

8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-20233
CVE	CVE-2020-27779
CVE	CVE-2020-25632
CVE	CVE-2020-14372
CVE	CVE-2020-25647
CVE	CVE-2020-27749
CVE	CVE-2021-20225

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/03, Modification date: 2021/03/12

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : grub2-2.02-26.40.1
Should be                : grub2-2.02-26.43.1
```

147564 - SUSE SLED15 / SLES15 Security Update : git (SUSE-SU-2021:0757-1)

Synopsis

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

Description

This update for git fixes the following issues :
On case-insensitive filesystems, with support for symbolic links, if Git is configured globally to apply delay-capable clean/smudge filters (such as Git LFS), Git could be fooled into running remote code during a clone. (bsc#1183026, CVE-2021-21300)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1183026

https://www.suse.com/security/cve/CVE-2021-21300/

http://www.nessus.org/u?7878754c

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :

zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-757=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-757=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-757=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-757=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-757=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-757=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-757=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-757=1
SUSE Linux Enterprise Module for Development Tools 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Development-Tools-15-SP3-2021-757=1
SUSE Linux Enterprise Module for Development Tools 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Development-Tools-15-SP2-2021-757=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-757=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-757=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-757=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-757=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-757=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-757=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-757=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.4

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE CVE-2021-21300

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/10, Modification date: 2021/03/18

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : git-core-2.26.2-3.28.2
Should be                : git-core-2.26.2-3.31.1
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/12/09, Modification date: 2020/03/09

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote operating system : Linux Kernel 4.12.14-8.58-azure on SuSE15.1
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 4.12.14-8.58-azure on SuSE15.1
```

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/19, Modification date: 2020/05/13

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
The following card manufacturers were identified :
```

```
00:0D:3A:3E:46:D8 : Microsoft Corp.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

See Also

Solution

Protect your target with an IP filter.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/04, Modification date: 2021/04/20

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Port 8443/tcp was found to be open
```

172.16.4.38 (TCP/22) Vulnerability State: Resurfaced

```
Port 22/tcp was found to be open
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/05/30, Modification date: 2020/06/12

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

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

The output of "uname -a" is :
Linux iplhrccd 4.12.14-8.58-azure #1 SMP Tue Jan 5 06:31:30 UTC 2021 (78ce6d4) x86_64 x86_64
 x86_64 GNU/Linux

The remote SuSE system is :
SUSE Linux Enterprise Server 15 SP1
PATCHLEVEL = 1

Local security checks have been enabled for this host.
```

```
Runtime : 12.125654 seconds
```

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.).

See Also

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/10/15, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Here is the list of packages installed on the remote SuSE Linux system :

  docker-19.03.11_ce-6.34.2|(none)
  efibootmgr-14-2.8|(none)
  libunwind-1.2.1-4.2.3|(none)
  python3-msrest-0.6.19-6.4.1|(none)
  vim-data-8.0.1568-5.6.1|(none)
  libmediacheck5-5.2-7.3.2|(none)
  python3-cryptography-2.1.4-4.6.1|(none)
  python3-msrestazure-0.6.4-6.4.1|(none)
  libnl3-200-3.3.0-1.29|(none)
  libcom_err2-1.43.8-4.23.1|(none)
  gvfs-backend-samba-1.34.2.1-4.13.1|(none)
  libelf1-0.168-4.5.3|(none)
  findutils-4.6.0-4.3.1|(none)
  libpcre1-8.41-4.20|(none)
  makedumpfile-1.6.3-10.6.1|(none)
  fillup-1.42-2.18|(none)
  hwinfo-21.70-3.6.1|(none)
  gptfdisk-1.0.1-2.11|(none)
  libsystemd0-234-24.64.1|(none)
  libp11-kit0-0.23.2-4.8.3|(none)
  libgraphite2-3-1.3.11-2.12|(none)
  findutils-lang-4.6.0-4.3.1|(none)
  yast2-bootloader-4.1.26-3.5.1|(none)
  libpsl5-0.20.1-1.20|(none)
  libsecret-1-0-0.18.7-1.15|(none)
  libisccfg160-9.11.2-12.13.2|(none)
  libldap-2_4-2-2.4.46-9.40.1|(none)
  python3-pydocumentdb-2.3.2-1.36|(none)
  libSM6-1.2.2-1.23|(none)
  perl-gettext-1.07-1.442|(none)
  libdevmapper-event1_03-1.02.149-12.37.1|(none)
  yast2-ldap-4.1.0-1.28|(none)
  sle-module-server-applications-release-15.1-66.1|(none)
  libthai0-0.1.27-1.16|(none)
  iscsiuio-0.7.8.2-13.37.1|(none)
  gtk3-data-3.22.30-4.19.1|(none)
  perl-Crypt-SmbHash-0.12-1.24|(none)
  libsoftokn3-3.53.1-3.51.1|(none)
  yast2-update-4.1.12-3.9.2|(none)
```

```
shadow-4.6-3.5.6|(none)
liblvm2cmd2_02-2.02.180-12.37.1|(none)
python3-azure-mgmt-servicefabric-0.2.0-4.22|(none)
yast2-perl-bindings-4.1.0-1.18|(none)
mozilla-nss-3.53.1-3.51.1|(none)
python3-azure-mgmt-rdbms-1.2.0-4.22|(none)
libhavege1-1.9.2-6.1|(none)
at-spi2-atk-common-2.26.3-4.3.5|(none)
parted-lang-3.2-11.14.1|(none)
python3-azure-mgmt-keyvault-1.1.0-5.22|(none)
zsh-5.6-5.17|(none)
liboauth0-1.0.3-3.34|(none)
python3-tabulate-0.7.7-1.18|(none)
grub2-x86_64-efi-2.02-26.40.1|(none)
python3-azure-mgmt-datalake-store-0.5.0-4.22|(none)
python3-distro-1.2.0-1.18|(none)
[...]
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS Base Score

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/07/02, Modification date: 2020/11/06

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

117887 - Local Checks Enabled

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enable local checks.

Description

Nessus was able to enable local checks because it was possible to log in to the remote host using provided credentials, the remote host was identified as an operating system or device for which local checks are available, and the necessary information was able to be obtained from the remote host in order to enable local checks.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/10/02, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Local checks have been enabled.

Account  : iplroot
Protocol : SSH
```

148162 - SUSE SLED15 / SLES15 Security Update : ruby2.5 (SUSE-SU-2021:0933-1)

Synopsis

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

Description

This update for ruby2.5 fixes the following issues :
CVE-2020-25613: Fixed a potential HTTP Request Smuggling in WEBrick (bsc#1177125).
Enable optimizations also on ARM64 (bsc#1177222)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1177125

https://bugzilla.suse.com/show_bug.cgi?id=1177222

https://www.suse.com/security/cve/CVE-2020-25613/

http://www.nessus.org/u?d248d1fb

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE MicroOS 5.0 :
zypper in -t patch SUSE-SUSE-MicroOS-5.0-2021-933=1
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-933=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-933=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-933=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-933=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-933=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-933=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-933=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-933=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-933=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-933=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :

zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-933=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-933=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-933=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-933=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-933=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2020-25613

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/26, Modification date: 2021/03/30

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libruby2_5-2_5-2.5.8-4.11.1
Should be                : libruby2_5-2_5-2.5.8-4.14.1

Remote package installed : ruby2.5-2.5.8-4.11.1
Should be                : ruby2.5-2.5.8-4.14.1

Remote package installed : ruby2.5-stdlib-2.5.8-4.11.1
Should be                : ruby2.5-stdlib-2.5.8-4.14.1
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/01, Modification date: 2021/02/03

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

148165 - SUSE SLES15 Security Update : gnutls (SUSE-SU-2021:0934-1)

Synopsis

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

Description

This update for gnutls fixes the following issues :
CVE-2021-20232: Fixed a use after free issue which could have led to memory corruption and other potential consequences (bsc#1183456).
CVE-2021-20231: Fixed a use after free issue which could have led to memory corruption and other potential consequences (bsc#1183457).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1183456

https://bugzilla.suse.com/show_bug.cgi?id=1183457

https://www.suse.com/security/cve/CVE-2021-20231/

https://www.suse.com/security/cve/CVE-2021-20232/

http://www.nessus.org/u?00132084

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-934=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-934=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-934=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-934=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-934=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-934=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-934=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-934=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-934=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-934=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-934=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-934=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-934=1

SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

8.4

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-20232
CVE	CVE-2021-20231

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/26, Modification date: 2021/03/30

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libgnutls30-3.6.7-6.37.1
Should be                : libgnutls30-3.6.7-6.40.2
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2002/03/06, Modification date: 2021/01/19

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

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

  - 1.99
```

- 2.0

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/01/06, Modification date: 2020/06/12

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
A TLSv1/TLSv11/TLSv12 server is listening on this port that requests a client certificate.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
 Subject Name:

Country: DE
Organization: SAP SE
Organization Unit: Connectivity
Common Name: SCC

Issuer Name:

Country: DE
Organization: SAP SE
Organization Unit: Connectivity
Common Name: SCC

Serial Number: 0E 19 B4 DC
```

```
Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 02 17:33:54 2015 GMT
Not Valid After: Oct 12 17:33:54 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A3 03 88 B6 46 3C 5E 2A 33 8D 04 11 71 24 5E 95 96 9C 1C
            1F F6 F3 93 CA 30 D0 FE 46 C8 88 BE FA 85 50 CB 4E 91 A3 C7
            B8 25 14 21 B8 02 1D DC A3 D5 F6 85 92 4D B3 F3 21 8A 20 87
            C4 CD 12 99 21 30 74 E3 3A 26 18 70 A9 09 FF E4 22 AB D3 8B
            30 A8 04 59 DC 88 9F F3 C0 92 88 90 C2 37 F6 8D F4 86 F8 72
            24 92 81 78 DD 08 34 7A B0 D7 2E 23 70 0F 55 3D BE A7 E4 A1
            E8 07 55 DD E2 7C 6D 91 43 33 FD 4C 01 5C 00 67 9D B3 61 E4
            1D C4 D0 6A 8F 15 34 44 57 D1 A9 1B D7 EF 06 06 E1 B3 F9 A8
            CF BA A6 66 B1 E0 20 69 62 15 17 95 50 CB D5 DE 9A 04 B8 EA
            4E 80 AF 8A 1E FC 86 50 63 BE F7 D4 5A 39 20 41 41 1F 82 11
            32 AC 8A 3F 11 03 43 76 3F BA 21 18 91 F9 55 D3 DC B9 15 41
            B0 4D 8C EB 73 56 59 29 06 47 9B 32 DD 0F 43 D0 D7 3D BF AB
            0D A2 0F 30 90 D8 00 90 C9 4F D7 ED 3F FE 2A 36 3F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 75 DB DA 35 14 67 3C 05 DD 78 89 C7 9E E5 39 EC B5 C6 17
           3A 76 0F 7C 8D 12 34 D5 F1 CD 21 04 5E C3 87 9F 4B 6A 25 5E
           BF 7C BA 6C BD FB D1 C0 44 22 FF 6D 51 4D CA 32 8A F0 A4 D4
           74 50 5A 26 6C D6 A5 35 2B 28 E2 34 EC 5A 10 8F 1D B7 40 C3
           1E C7 5D DD C4 6A 2A F6 0B B9 DD B2 50 2C 12 39 F8 E3 62 85
           11 25 4D 36 20 27 DF 5F D1 EF F7 8D 06 55 D3 76 BD 60 BE D0
           99 C4 FA 9E 7F 3E 5D 0B 01 48 A7 4E 80 02 65 98 E4 76 FC 73
           B4 FB 43 00 0D E0 28 94 CE 9C 31 2E 7E F0 22 01 43 3B 6D A6
           FD E8 77 FF 97 33 [...]
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0535

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/06/18, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
  URL     : https://172.16.4.38:8443/
  Version : unknown
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/10/16, Modification date: 2020/05/13

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
The following is a consolidated list of detected MAC addresses:
  - 00:0D:3A:3E:46:D8
```

146576 - SUSE SLED15 / SLES15 Security Update : screen (SUSE-SU-2021:0492-1)

Synopsis

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

Description

This update for screen fixes the following issues :
CVE-2021-26937: Fixed double width combining char handling that could lead to a denial of service or code execution (bsc#1182092).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182092

https://www.suse.com/security/cve/CVE-2021-26937/

http://www.nessus.org/u?2d13ee3d

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-492=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-492=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-492=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-492=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-492=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-492=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-492=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-492=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :

zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-492=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-492=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-492=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-492=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-492=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-492=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-492=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE CVE-2021-26937

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/02/18, Modification date: 2021/02/22

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : screen-4.6.2-3.14
Should be                : screen-4.6.2-5.3.1
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

See Also

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2012/01/17, Modification date: 2020/04/27

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=DE/O=SAP SE/OU=Connectivity/CN=SCC
```

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'.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVB:0001-B-0507

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/08/01, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Login account : iplroot
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 /usr/sbin/dmidecode"
      Response : "# dmidecode 3.2\nScanning /dev/mem for entry point."
      Error    : "/sys/firmware/dmi/tables/smbios_entry_point: Permission denied\n/dev/mem:
 Permission denied"
  - Plugin Filename : host_tag_nix.nbin
    Plugin ID       : 87414
```

```
    Plugin Name     : Host Tagging (Linux)
    - Command  : "sh -c \"echo 57150ab59c7541c1bf96082f22d5fa0b > /etc/tenable_tag && echo OK\""
      Response : null
      Error    : "sh: /etc/tenable_tag: Permission denied"
  - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
    Plugin ID       : 125216
    Plugin Name     : Processor Speculative Execution Vulnerabilities (Linux)
    - Command  : "cat /sys/kernel/debug/x86/pti_enabled"
      Response : null
      Error    : "cat: /sys/kernel/debug/x86/pti_enabled: Permission denied"
    - Command  : "cat /sys/kernel/debug/x86/retp_enabled"
      Response : null
      Error    : "cat: /sys/kernel/debug/x86/retp_enabled: Permission denied"
    - Command  : "cat /sys/kernel/debug/x86/ibrs_enabled"
      Response : null
      Error    : "cat: /sys/kernel/debug/x86/ibrs_enabled: 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    : "cat: /etc/shadow: Permission denied"
  - Plugin Filename : unix_compliance_check.nbin
    Plugin ID       : 21157
    Plugin Name     : Unix Compliance Checks
    - Command  : "LANG=C; cat '/boot/grub2/grub.cfg'|cat"
      Response : null
      Error    : "cat: \n/boot/grub2/grub.cfg: Permission denied"
    - Command  : "LANG=C; cat '/boot/grub2/grub.cfg'|cat"
      Response : [...]
```

148151 - SUSE SLES15 Security Update : libzypp, zypper (SUSE-SU-2021:0956-1)

Synopsis

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

Description

This update for libzypp, zypper fixes the following issues :
Update zypper to version 1.14.43 :
doc: give more details about creating versioned package locks (bsc#1181622)
man: Document synonymously used patch categories (bsc#1179847)
Fix source-download commands help (bsc#1180663)
man: Recommend to use the --non-interactive global option rather than the command option -y (bsc#1179816)
Extend apt packagemap (fixes #366)
--quiet: Fix install summary to write nothing if there's nothing todo (bsc#1180077)
Prefer /run over /var/run.
Update libzypp to 17.25.8 :
Try to provide a mounted /proc in --root installs (bsc#1181328) Some systemd tools require /proc to be mounted and fail if it's not there.
Enable release packages to request a releaxed suse/opensuse vendorcheck in dup when migrating. (bsc#1182629)
Patch: Identify well-known category names (bsc#1179847) This allows to use the RH and SUSE patch categrory names synonymously: (recommended = bugfix) and (optional = feature = enhancement).
Add missing includes for GCC 11 compatibility.
Fix %posttrans script execution (fixes #265) The scripts are execuable. No need to call them through 'sh -c'.
Commit: Fix rpmdb compat symlink in case rpm got removed.
Repo: Allow multiple baseurls specified on one line (fixes #285)
Regex: Fix memory leak and undefined behavior.
Add rpm buildrequires for test suite (fixes #279)
Use rpmdb2solv new -D switch to tell the location ob the rpmdatabase to use.
CVE-2017-9271: Fixed information leak in the log file (bsc#1050625 bsc#1177583)
RepoManager: Force refresh if repo url has changed (bsc#1174016)
RepoManager: Carefully tidy up the caches. Remove non-directory entries. (bsc#1178966)
RepoInfo: ignore legacy type= in a .repo file and let RepoManager probe (bsc#1177427).
RpmDb: If no database exists use the _dbpath configured in rpm. Still makes sure a compat symlink at /var/lib/rpm exists in case the configures _dbpath is elsewhere. (bsc#1178910)
Fixed update of gpg keys with elongated expire date (bsc#1179222)
needreboot: remove udev from the list (bsc#1179083)
Fix lsof monitoring (bsc#1179909)
Rephrase solver problem descriptions (jsc#SLE-8482)
Adapt to changed gpg2/libgpgme behavior (bsc#1180721)
Multicurl backend breaks with with unknown filesize (fixes #277)

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

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1050625

https://bugzilla.suse.com/show_bug.cgi?id=1174016

https://bugzilla.suse.com/show_bug.cgi?id=1177238

https://bugzilla.suse.com/show_bug.cgi?id=1177275

https://bugzilla.suse.com/show_bug.cgi?id=1177427

https://bugzilla.suse.com/show_bug.cgi?id=1177583

https://bugzilla.suse.com/show_bug.cgi?id=1178910

https://bugzilla.suse.com/show_bug.cgi?id=1178966

https://bugzilla.suse.com/show_bug.cgi?id=1179083

https://bugzilla.suse.com/show_bug.cgi?id=1179222

https://bugzilla.suse.com/show_bug.cgi?id=1179909

https://www.suse.com/security/cve/CVE-2017-9271/

https://bugzilla.suse.com/show_bug.cgi?id=1179847

https://bugzilla.suse.com/show_bug.cgi?id=1181328

https://bugzilla.suse.com/show_bug.cgi?id=1181622

https://bugzilla.suse.com/show_bug.cgi?id=1182629

https://bugzilla.suse.com/show_bug.cgi?id=1179816

https://bugzilla.suse.com/show_bug.cgi?id=1180077

https://bugzilla.suse.com/show_bug.cgi?id=1180663

https://bugzilla.suse.com/show_bug.cgi?id=1180721

http://www.nessus.org/u?dd8b693b

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-956=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-956=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-956=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-956=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-956=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-956=1
SUSE Linux Enterprise Installer 15-SP1 :
zypper in -t patch SUSE-SLE-INSTALLER-15-SP1-2021-956=1

SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-956=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-956=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-956=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

1.4

CVSS v3.0 Base Score

3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

2.9 (E:U/RL:O/RC:C)

CVSS Base Score

2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

1.6 (E:U/RL:OF/RC:C)

References

CVE CVE-2017-9271

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/26, Modification date: 2021/03/30

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libsigc-2_0-0-2.10.0-3.5.1
Should be                : libsigc-2_0-0-2.10.0-3.7.1

Remote package installed : libsolv-tools-0.7.16-3.29.2
Should be                : libsolv-tools-0.7.17-3.32.1

Remote package installed : libyui-ncurses-pkg9-2.48.9-7.5.8
Should be                : libyui-ncurses-pkg9-2.48.9-7.7.1

Remote package installed : libzypp-17.25.1-3.34.10
Should be                : libzypp-17.25.8-3.48.1

Remote package installed : python3-solv-0.7.16-3.29.2
Should be                : python3-solv-0.7.17-3.32.1

Remote package installed : yast2-pkg-bindings-4.1.3-3.8.8
Should be                : yast2-pkg-bindings-4.1.3-3.10.3

Remote package installed : zypper-1.14.40-3.25.10
Should be                : zypper-1.14.43-3.34.1
```

146615 - SUSE SLED15 / SLES15 Security Update : bind (SUSE-SU-2021:0507-1)

Synopsis

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

Description

This update for bind fixes the following issues :

CVE-2020-8625: A vulnerability in BIND's GSSAPI security policy negotiation can be targeted by a buffer overflow attack [bsc#1182246]
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182246

https://www.suse.com/security/cve/CVE-2020-8625/

http://www.nessus.org/u?55d76626

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-507=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-507=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-507=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-507=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-507=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-507=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-507=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-507=1
SUSE Linux Enterprise Module for Server Applications 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Server-Applications-15-SP2-2021-507=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-507=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-507=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-507=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-507=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-507=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-507=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.7

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2020-8625

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/02/19, Modification date: 2021/03/02

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : bind-utils-9.16.6-12.38.1
Should be                : bind-utils-9.16.6-12.41.1

Remote package installed : libbind9-1600-9.16.6-12.38.1
Should be                : libbind9-1600-9.16.6-12.41.1

Remote package installed : libdns1605-9.16.6-12.38.1
Should be                : libdns1605-9.16.6-12.41.1

Remote package installed : libirs1601-9.16.6-12.38.1
Should be                : libirs1601-9.16.6-12.41.1

Remote package installed : libisc1606-9.16.6-12.38.1
Should be                : libisc1606-9.16.6-12.41.1

Remote package installed : libiscсc1600-9.16.6-12.38.1
Should be                : libiscсc1600-9.16.6-12.41.1

Remote package installed : libisccfg1600-9.16.6-12.38.1
Should be                : libisccfg1600-9.16.6-12.41.1

Remote package installed : libns1604-9.16.6-12.38.1
Should be                : libns1604-9.16.6-12.41.1
```

147570 - SUSE SLED15 / SLES15 Security Update : openldap2 (SUSE-SU-2021:0723-1)

Synopsis

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

Description

This update for openldap2 fixes the following issues :
bsc#1182408 CVE-2020-36230 - an assertion failure in slapd in the X.509 DN parsing in decode.c ber_next_element, resulting in denial of service.
bsc#1182411 CVE-2020-36229 - ldap_X509dn2bv crash in the X.509 DN parsing in ad_keystring, resulting in denial of service.
bsc#1182412 CVE-2020-36228 - integer underflow leading to crash in the Certificate List Exact Assertion processing, resulting in denial of service.
bsc#1182413 CVE-2020-36227 - infinite loop in slapd with the cancel_extop Cancel operation, resulting in denial of service.
bsc#1182416 CVE-2020-36225 - double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.
bsc#1182417 CVE-2020-36224 - invalid pointer free and slapd crash in the saslAuthzTo processing, resulting in denial of service.
bsc#1182415 CVE-2020-36226 - memch->bv_len miscalculation and slapd crash in the saslAuthzTo processing, resulting in denial of service.
bsc#1182419 CVE-2020-36222 - assertion failure in slapd in the saslAuthzTo validation, resulting in denial of service.
bsc#1182420 CVE-2020-36221 - slapd crashes in the Certificate Exact Assertion processing, resulting in denial of service (schema_init.c serialNumberAndIssuerCheck).
bsc#1182418 CVE-2020-36223 - slapd crash in the Values Return Filter control handling, resulting in denial of service (double free and out-of-bounds read).
bsc#1182279 CVE-2021-27212 - an assertion failure in slapd can occur in the issuerAndThisUpdateCheck function via a crafted packet, resulting in a denial of service (daemon exit) via a short timestamp.
This is related to schema_init.c and checkTime.

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

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182279

https://bugzilla.suse.com/show_bug.cgi?id=1182408

https://bugzilla.suse.com/show_bug.cgi?id=1182411

https://bugzilla.suse.com/show_bug.cgi?id=1182412

https://bugzilla.suse.com/show_bug.cgi?id=1182413

https://bugzilla.suse.com/show_bug.cgi?id=1182415

https://bugzilla.suse.com/show_bug.cgi?id=1182416

https://bugzilla.suse.com/show_bug.cgi?id=1182417

https://bugzilla.suse.com/show_bug.cgi?id=1182418

https://bugzilla.suse.com/show_bug.cgi?id=1182419

https://bugzilla.suse.com/show_bug.cgi?id=1182420

https://www.suse.com/security/cve/CVE-2020-36221/

https://www.suse.com/security/cve/CVE-2020-36222/

https://www.suse.com/security/cve/CVE-2020-36223/

https://www.suse.com/security/cve/CVE-2020-36224/

https://www.suse.com/security/cve/CVE-2020-36225/

https://www.suse.com/security/cve/CVE-2020-36226/

https://www.suse.com/security/cve/CVE-2020-36227/

https://www.suse.com/security/cve/CVE-2020-36228/

https://www.suse.com/security/cve/CVE-2020-36229/

https://www.suse.com/security/cve/CVE-2020-36230/

https://www.suse.com/security/cve/CVE-2021-27212/

http://www.nessus.org/u?e321c48a

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-723=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-723=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-723=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-723=1
SUSE Linux Enterprise Server for SAP 15 :

zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-723=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-723=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-723=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-723=1
SUSE Linux Enterprise Module for Legacy Software 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Legacy-15-SP3-2021-723=1
SUSE Linux Enterprise Module for Legacy Software 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Legacy-15-SP2-2021-723=1
SUSE Linux Enterprise Module for Development Tools 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Development-Tools-15-SP3-2021-723=1
SUSE Linux Enterprise Module for Development Tools 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Development-Tools-15-SP2-2021-723=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-723=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-723=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-723=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-723=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-723=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-723=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-723=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.1

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-36222
CVE	CVE-2020-36221
CVE	CVE-2020-36224
CVE	CVE-2020-36223
CVE	CVE-2020-36226
CVE	CVE-2020-36225

CVE	CVE-2020-36228
CVE	CVE-2020-36227
CVE	CVE-2020-36229
CVE	CVE-2021-27212
CVE	CVE-2020-36230
XREF	IAVB:2021-B-0014

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/10, Modification date: 2021/04/05

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libldap-2_4-2-2.4.46-9.40.1
Should be                : libldap-2_4-2-2.4.46-9.48.1

Remote package installed : openldap2-client-2.4.46-9.40.1
Should be                : openldap2-client-2.4.46-9.48.1
```

146975 - SUSE SLED15 / SLES15 Security Update : bind (SUSE-SU-2021:0689-1)

Synopsis

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

Description

This update for bind fixes the following issues :
dnssec-keygen can no longer generate HMAC keys. Use tsig-keygen instead. [bsc#1180933]
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1180933

http://www.nessus.org/u?8ecd7d9f

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-689=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-689=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-689=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-689=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-689=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-689=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-689=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-689=1
SUSE Linux Enterprise Module for Server Applications 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Server-Applications-15-SP2-2021-689=1

SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-689=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-689=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-689=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-689=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-689=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-689=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/03/03, Modification date: 2021/03/03

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : bind-utils-9.16.6-12.38.1
Should be                : bind-utils-9.16.6-12.44.1

Remote package installed : libbind9-1600-9.16.6-12.38.1
Should be                : libbind9-1600-9.16.6-12.44.1

Remote package installed : libdns1605-9.16.6-12.38.1
Should be                : libdns1605-9.16.6-12.44.1

Remote package installed : libirs1601-9.16.6-12.38.1
Should be                : libirs1601-9.16.6-12.44.1

Remote package installed : libisc1606-9.16.6-12.38.1
Should be                : libisc1606-9.16.6-12.44.1

Remote package installed : libisccc1600-9.16.6-12.38.1
Should be                : libisccc1600-9.16.6-12.44.1

Remote package installed : libisccfg1600-9.16.6-12.38.1
Should be                : libisccfg1600-9.16.6-12.44.1

Remote package installed : libns1604-9.16.6-12.38.1
Should be                : libns1604-9.16.6-12.44.1
```

147741 - SUSE SLED15 / SLES15 Security Update : python (SUSE-SU-2021:0768-1)

Synopsis

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

Description

This update for python fixes the following issues :
python27 was upgraded to 2.7.18
CVE-2021-23336: Fixed a potential web cache poisoning by using a semicolon in query parameters use of semicolon as a query string separator (bsc#1182379).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182379

https://www.suse.com/security/cve/CVE-2021-23336/

http://www.nessus.org/u?d2139788

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-768=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-768=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-768=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-768=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-768=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-768=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-768=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-768=1
SUSE Linux Enterprise Module for Python2 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Python2-15-SP3-2021-768=1
SUSE Linux Enterprise Module for Python2 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Python2-15-SP2-2021-768=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP3-2021-768=1
SUSE Linux Enterprise Module for Desktop Applications 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Desktop-Applications-15-SP2-2021-768=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-768=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-768=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-768=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-768=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-768=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-768=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-768=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.0

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (E:U/RL:O/RC:C)

CVSS Base Score

4.0 (AV:N/AC:H/Au:N/C:N/I:P/A:P)

CVSS Temporal Score

3.0 (E:U/RL:OF/RC:C)

References

CVE CVE-2021-23336

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/12, Modification date: 2021/03/16

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libpython2_7-1_0-2.7.17-7.47.1
Should be                : libpython2_7-1_0-2.7.18-7.55.1

Remote package installed : python-2.7.17-7.47.1
Should be                : python-2.7.18-7.55.1

Remote package installed : python-base-2.7.17-7.47.1
Should be                : python-base-2.7.18-7.55.1

Remote package installed : python-xml-2.7.17-7.47.1
Should be                : python-xml-2.7.18-7.55.1
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/08/19, Modification date: 2021/04/14

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
A TLSv1 server answered on this port.


A web server is running on this port through TLSv1.
```

172.16.4.38 (TCP/22) Vulnerability State: Resurfaced

```
An SSH server is running on this port.
```

148304 - SUSE SLED15 / SLES15 Security Update : MozillaFirefox (SUSE-SU-2021:1007-1)

Synopsis

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

Description

This update for MozillaFirefox fixes the following issues :
Firefox was updated to 78.9.0 ESR (MFSA 2021-11, bsc#1183942)
- CVE-2021-23981: Texture upload into an unbound backing buffer resulted in an out-of-bound read

- CVE-2021-23982: Internal network hosts could have been probed by a malicious webpage
- CVE-2021-23984: Malicious extensions could have spoofed popup information
- CVE-2021-23987: Memory safety bugs
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1183942

https://www.suse.com/security/cve/CVE-2021-23981/

https://www.suse.com/security/cve/CVE-2021-23982/

https://www.suse.com/security/cve/CVE-2021-23984/

https://www.suse.com/security/cve/CVE-2021-23987/

http://www.nessus.org/u?b7e158dd

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE MicroOS 5.0 :
zypper in -t patch SUSE-SUSE-MicroOS-5.0-2021-1007=1
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-1007=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-1007=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-1007=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-1007=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-1007=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-1007=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-1007=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-1007=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-1007=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-1007=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-1007=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1007=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1007=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-1007=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

7.4

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-23987
CVE	CVE-2021-23981
CVE	CVE-2021-23982
CVE	CVE-2021-23984
XREF	IAVA:2021-A-0144

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/04/02, Modification date: 2021/04/08

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : mozilla-nspr-4.25.1-3.15.2
Should be                : mozilla-nspr-4.25.1-3.17.1
```

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/16, Modification date: 2019/03/06

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

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 and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/01/30, Modification date: 2019/11/22

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Apache-Coyote/1.1
  Cache-Control: private
  Expires: Thu, 01 Jan 1970 00:00:00 GMT
  Set-Cookie: JSESSIONID=CDBE605EFF70BA66B87FC7C5ABE5BFC577F361C4316E3051F4663E731ADA8CF0; Path=/;
 Secure; HttpOnly
  Content-Security-Policy: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval';
 connect-src 'self'; img-src 'self' data:; font-src 'self'; style-src 'self' 'unsafe-inline';
 frame-src 'self';
  X-Content-Security-Policy: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval';
 connect-src 'self'; img-src 'self' data:; font-src 'self'; style-src 'self' 'unsafe-inline';
 frame-src 'self';
  X-Frame-Options: DENY
  Content-Type: text/html;charset=UTF-8
  Content-Length: 4178
  vary: accept-encoding
  Date: Mon, 03 May 2021 06:42:29 GMT
  Connection: close

Response Body :



<!DOCTYPE html>
<html style="height: 98%">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<title>Login</title>
<script src="/resources/sap-ui-core.js" type="text/javascript" data-sap-ui-
libs="sap.m,sap.ui.layout" data-sap-ui-theme="sap_belize">
</script>
<style type="text/css">
.sapUiTheme-sap_belize #loginDiv {
 width: 400px;
 margin: 0 auto;
 padding: 10px;
 background-color: rgba(255, 255, 255, 0.5);
 border-radius: 15px;
}

.sapUiTheme-sap_belize .title {
```

```
 font-size: 2.5em;
 padding: 5px;
 color: #2b3f7b;
}

.sapUiTheme-sap_belize .label {
 color: #333333;
 margin-top: 0.4rem;
}

.sapUiTheme-sap_belize .sccLogin {
 background: url('/images/loginbg.jpg');
}

.sapUiTheme-sap_belize .helpBtn.sapMBtn>.sapMBtnTransparent>.sapMBtnIcon
 {
 color: #2b3f7b;
}
</style>
<script type="text/javascript">
sap.ui.getCore().getConfiguration().setLanguage('en-US');
var msgStrip = new sap.m.MessageStrip({
 visible:false,
 text:'User authentication [...]
```

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/04/21, Modification date: 2021/04/20

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :

  cpe:/o:novell:suse_linux:15.1

Following application CPE's matched on the remote system :

  cpe:/a:apache:tomcat:
  cpe:/a:openbsd:openssh:7.9
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/06/30, Modification date: 2021/04/20

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Hostname : iplhrccd
  iplhrccd (hostname command)
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
MAC
    ----------------------        ----------       ---           ----      --------------------
---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA       AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA       AES-CBC(256)
SHA1
```

```
   ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH          RSA      AES-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67      DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B      DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH          RSA      AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

146460 - SUSE SLES15 Security Update : containerd, docker, docker-runc, golang-github-docker-libnetwork (SUSE-SU-2021:0435-1)

Synopsis

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

Description

This update for containerd, docker, docker-runc, golang-github-docker-libnetwork fixes the following issues :
Security issues fixed :
CVE-2020-15257: Fixed a privilege escalation in containerd (bsc#1178969).
CVE-2021-21284: potential privilege escalation when the root user in the remapped namespace has access to the host filesystem (bsc#1181732)
CVE-2021-21285: pulling a malformed Docker image manifest crashes the dockerd daemon (bsc#1181730)
Non-security issues fixed :
Update Docker to 19.03.15-ce. See upstream changelog in the packaged /usr/share/doc/packages/docker/CHANGELOG.md. This update includes fixes for bsc#1181732 (CVE-2021-21284) and bsc#1181730 (CVE-2021-21285).
Only apply the boo#1178801 libnetwork patch to handle firewalld on openSUSE. It appears that SLES doesn't like the patch. (bsc#1180401)
Update to containerd v1.3.9, which is needed for Docker v19.03.14-ce and fixes CVE-2020-15257. bsc#1180243
Update to containerd v1.3.7, which is required for Docker 19.03.13-ce.
bsc#1176708
Update to Docker 19.03.14-ce. See upstream changelog in the packaged /usr/share/doc/packages/docker/CHANGELOG.md. CVE-2020-15257 bsc#1180243 https://github.com/docker/docker-ce/releases/tag/v19.03.14
Enable fish-completion
Add a patch which makes Docker compatible with firewalld with nftables backend. Backport of https://github.com/moby/libnetwork/pull/2548 (bsc#1178801, SLE-16460)
Update to Docker 19.03.13-ce. See upstream changelog in the packaged /usr/share/doc/packages/docker/CHANGELOG.md. bsc#1176708
Fixes for %_libexecdir changing to /usr/libexec (bsc#1174075)
Emergency fix: %requires_eq does not work with provide symbols, only effective package names. Convert back to regular Requires.
Update to Docker 19.03.12-ce. See upstream changelog in the packaged /usr/share/doc/packages/docker/CHANGELOG.md.
Use Go 1.13 instead of Go 1.14 because Go 1.14 can cause all sorts of spurrious errors due to Go returning -EINTR from I/O syscalls much more often (due to Go 1.14's pre-emptive goroutine support).
Add BuildRequires for all -git dependencies so that we catch missing dependencies much more quickly.
Update to libnetwork 55e924b8a842, which is required for Docker 19.03.14-ce. bsc#1180243
Add patch which makes libnetwork compatible with firewalld with nftables backend. Backport of https://github.com/moby/libnetwork/pull/2548 (bsc#1178801, SLE-16460)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1174075

https://bugzilla.suse.com/show_bug.cgi?id=1176708

https://bugzilla.suse.com/show_bug.cgi?id=1178801

https://bugzilla.suse.com/show_bug.cgi?id=1178969

https://bugzilla.suse.com/show_bug.cgi?id=1180243

https://bugzilla.suse.com/show_bug.cgi?id=1180401

https://bugzilla.suse.com/show_bug.cgi?id=1181730

https://bugzilla.suse.com/show_bug.cgi?id=1181732

https://github.com/docker/docker-ce/releases/tag/v19.03.14

https://github.com/moby/libnetwork/pull/2548

https://www.suse.com/security/cve/CVE-2020-15257/

https://www.suse.com/security/cve/CVE-2021-21284/

https://www.suse.com/security/cve/CVE-2021-21285/

http://www.nessus.org/u?fccb77db

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-435=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-435=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-435=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-435=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-435=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-435=1
SUSE Linux Enterprise Module for Containers 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Containers-15-SP3-2021-435=1
SUSE Linux Enterprise Module for Containers 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Containers-15-SP2-2021-435=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-435=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-435=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-435=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

6.3

CVSS v3.0 Base Score

5.2 (AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)

CVSS v3.0 Temporal Score

4.5 (E:U/RL:O/RC:C)

CVSS Base Score

3.6 (AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSS Temporal Score

2.7 (E:U/RL:OF/RC:C)

References

CVE	CVE-2021-21285
CVE	CVE-2021-21284
CVE	CVE-2020-15257

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/02/12, Modification date: 2021/02/16

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : containerd-1.2.13-5.22.2
Should be                : containerd-1.3.9-5.29.3

Remote package installed : docker-19.03.11_ce-6.34.2
Should be                : docker-19.03.15_ce-6.43.3

Remote package installed : docker-libnetwork-0.7.0.1+gitr2902_153d0769a118-4.21.2
Should be                : docker-libnetwork-0.7.0.1+gitr2908_55e924b8a842-4.28.3

Remote package installed : docker-runc-1.0.0rc10+gitr3981_dc9208a3303f-6.38.2
Should be                : docker-runc-1.0.0rc10+gitr3981_dc9208a3303f-6.45.3
```

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.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

```
SSH version : SSH-2.0-OpenSSH_7.9
```

```
SSH supported authentication : publickey,password,keyboard-interactive
```

149077 - SUSE SLED15 / SLES15 Security Update : libnettle (SUSE-SU-2021:1412-1)

Synopsis

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

Description

This update for libnettle fixes the following issues :
CVE-2021-20305: Fixed the multiply function which was being called with out-of-range scalars (bsc#1184401).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1184401

https://www.suse.com/security/cve/CVE-2021-20305/

http://www.nessus.org/u?7170e887

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE MicroOS 5.0 :
zypper in -t patch SUSE-SUSE-MicroOS-5.0-2021-1412=1
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-1412=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-1412=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-1412=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-1412=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-1412=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-1412=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-1412=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-1412=1
SUSE Linux Enterprise Module for Basesystem 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP3-2021-1412=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-1412=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-1412=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-1412=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1412=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1412=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-1412=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

5.9

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

CVE CVE-2021-20305

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/04/29, Modification date: 2021/04/29

Ports

172.16.4.38 (TCP/0) Vulnerability State: New

```
Remote package installed : libhogweed4-3.4.1-4.12.1
Should be                : libhogweed4-3.4.1-4.15.1

Remote package installed : libnettle6-3.4.1-4.12.1
Should be                : libnettle6-3.4.1-4.15.1
```

148175 - SUSE SLED15 / SLES15 Security Update : ldb (SUSE-SU-2021:0944-1)

Synopsis

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

Description

This update for ldb fixes the following issues :
CVE-2020-27840: Fixed an unauthenticated remote heap corruption via bad DNs (bsc#1183572).
CVE-2021-20277: Fixed an out of bounds read in ldb_handler_fold (bsc#1183574).
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1183572

https://bugzilla.suse.com/show_bug.cgi?id=1183574

https://www.suse.com/security/cve/CVE-2020-27840/

https://www.suse.com/security/cve/CVE-2021-20277/

http://www.nessus.org/u?481ed88d

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-944=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-944=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-944=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-944=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-944=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-944=1
SUSE Linux Enterprise Module for Python2 15-SP3 :
zypper in -t patch SUSE-SLE-Module-Python2-15-SP3-2021-944=1
SUSE Linux Enterprise Module for Python2 15-SP2 :

zypper in -t patch SUSE-SLE-Module-Python2-15-SP2-2021-944=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-944=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-944=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-944=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.0

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-20277
CVE	CVE-2020-27840
XREF	IAVA:2021-A-0140

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/26, Modification date: 2021/04/01

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libldb1-1.4.6-3.5.2
Should be                : libldb1-1.4.6-3.8.1

Remote package installed : python3-ldb-1.4.6-3.5.2
Should be                : python3-ldb-1.4.6-3.8.1
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption
MAC
    ----------------------        ----------        ---           ----     ---------------------
---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

147060 - SUSE SLES15 Security Update : python-cryptography (SUSE-SU-2021:0696-1)

Synopsis

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

Description

This update for python-cryptography fixes the following issues :
CVE-2020-36242: Using the Fernet class to symmetrically encrypt multi gigabyte values could result in an integer overflow and buffer overflow (bsc#1182066).

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

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182066

https://www.suse.com/security/cve/CVE-2020-36242/

http://www.nessus.org/u?bb019bb8

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-696=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-696=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-696=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-696=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-696=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-696=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-696=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-696=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-696=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-696=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-696=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-696=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-696=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.0

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE CVE-2020-36242

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/04, Modification date: 2021/03/08

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : python3-cryptography-2.1.4-4.6.1
Should be                : python3-cryptography-2.1.4-4.9.2
```

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.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2000/01/04, Modification date: 2020/10/30

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
The remote web server type is :

Apache-Coyote/1.1
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/09/08, Modification date: 2020/09/22

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Version      : 7.0
```

```
Vendor       : Microsoft Corporation
Release Date : 12/07/2018
UUID         : ae98417d-a961-0346-85c0-57f1f528ca5e
Secure boot  : disabled
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :
```

```
  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/10/15, Modification date: 2020/10/15

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

```
Nessus was able to log in to the remote host via the following
protocol as iplroot :

  Protocol        : SSH
  Port            : 22
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/06/12, Modification date: 2021/02/04

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
 USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.1  0.0  72856  8840 ?        Ss   08:45   0:20 /usr/lib/systemd/systemd --
switched-root --system --deserialize 23
root          2  0.0  0.0      0     0 ?        S    08:45   0:00 [kthreadd]
root          4  0.0  0.0      0     0 ?        S<   08:45   0:00 [kworker/0:0H]
root          6  0.0  0.0      0     0 ?        S<   08:45   0:00 [mm_percpu_wq]
root          7  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/0]
root          8  0.0  0.0      0     0 ?        S    08:45   0:02 [rcu_sched]
root          9  0.0  0.0      0     0 ?        S    08:45   0:00 [rcu_bh]
root         10  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/0]
root         11  0.0  0.0      0     0 ?        S    08:45   0:00 [watchdog/0]
root         12  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/0]
root         13  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/1]
root         14  0.0  0.0      0     0 ?        S    08:45   0:00 [watchdog/1]
root         15  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/1]
root         16  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/1]
root         18  0.0  0.0      0     0 ?        S<   08:45   0:00 [kworker/1:0H]
root         19  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/2]
root         20  0.0  0.0      0     0 ?        S    08:45   0:00 [watchdog/2]
root         21  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/2]
root         22  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/2]
root         24  0.0  0.0      0     0 ?        S<   08:45   0:00 [kworker/2:0H]
root         25  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/3]
root         26  0.0  0.0      0     0 ?        S    08:45   0:00 [watchdog/3]
root         27  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/3]
root         28  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/3]
root         30  0.0  0.0      0     0 ?        S<  [...]
```

148143 - SUSE SLES15 Security Update : nghttp2 (SUSE-SU-2021:0931-1)

Synopsis

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

Description

This update for nghttp2 fixes the following issues :
CVE-2020-11080: HTTP/2 Large Settings Frame DoS (bsc#1181358)

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

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1172442

https://www.suse.com/security/cve/CVE-2020-11080/

https://bugzilla.suse.com/show_bug.cgi?id=1181358

http://www.nessus.org/u?b1a9f07f

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-931=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-931=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-931=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-931=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-931=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-931=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-931=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-931=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-931=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-931=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-931=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-931=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-931=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE CVE-2020-11080

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/26, Modification date: 2021/03/30

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libnghttp2-14-1.40.0-3.6.3
Should be                : libnghttp2-14-1.40.0-3.11.1
```

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.

See Also

Solution

Install the patches listed below.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/07/08, Modification date: 2021/04/20

Ports

172.16.4.38 (TCP/0) Vulnerability State: Resurfaced

```
. You need to take the following 21 actions :


[ SUSE SLED15 / SLES15 Security Update : MozillaFirefox (SUSE-SU-2021:1007-1) (148304) ]

+ Action to take : To install this SUSE Security Update use the SUSE recommended installation
 methods like YaST online_update or 'zypper patch'.

Alternatively you can run the command listed for your product :

SUSE MicroOS 5.0 :

zypper in -t patch SUSE-SUSE-MicroOS-5.0-2021-1007=1

SUSE Manager Server 4.0 :

zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-1007=1

SUSE Manager Retail Branch Server 4.0 :

zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-1007=1

SUSE Manager Proxy 4.0 :

zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-1007=1

SUSE Linux Enterprise Server for SAP 15-SP1 :
```

```
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-1007=1

SUSE Linux Enterprise Server for SAP 15 :

zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-1007=1

SUSE Linux Enterprise Server 15-SP1-LTSS :

zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-1007=1

SUSE Linux Enterprise Server 15-SP1-BCL :

zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-1007=1

SUSE Linux Enterprise Server 15-LTSS :

zypper in -t patch SUSE-SLE-Product-SLES-15-2021-1007=1

SUSE Linux Enterprise Module for Basesystem 15-SP2 :

zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-1007=1

SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :

zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-1007=1

SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :

zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-1007=1

SUSE Linux Enterprise High Performance Computing 15-LTSS :

zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1007=1

SUSE Linux Enterprise High Performance Computing 15-ESPOS :

zypper in -t patch SUSE-SLE-Product-HPC-15-2021-1007=1

SUSE Enterprise Storage 6 :

zypper in -t patch SUSE-Storage-6-2021-1007=1

SUSE CaaS Platform 4.0 :

To install this update, use the SUSE CaaS [...]
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/11/22, Modification date: 2020/03/31

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
TLSv1 is enabled and the server supports at least one cipher.
```

146903 - SUSE SLED15 / SLES15 Security Update : glibc (SUSE-SU-2021:0653-1)

Synopsis

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

Description

This update for glibc fixes the following issues :
Fix buffer overrun in EUC-KR conversion module (CVE-2019-25013, bsc#1182117, BZ #24973)
x86: Harden printf against non-normal long double values (CVE-2020-29573, bsc#1179721, BZ #26649)
gconv: Fix assertion failure in ISO-2022-JP-3 module (CVE-2021-3326, bsc#1181505, BZ #27256)
iconv: Accept redundant shift sequences in IBM1364 (CVE-2020-27618, bsc#1178386, BZ #26224)
iconv: Fix incorrect UCS4 inner loop bounds (CVE-2020-29562, bsc#1179694, BZ #26923)
Fix parsing of /sys/devices/system/cpu/online (bsc#1180038, BZ #25859)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1178386

https://bugzilla.suse.com/show_bug.cgi?id=1179694

https://bugzilla.suse.com/show_bug.cgi?id=1179721

https://bugzilla.suse.com/show_bug.cgi?id=1180038

https://bugzilla.suse.com/show_bug.cgi?id=1181505

https://bugzilla.suse.com/show_bug.cgi?id=1182117

https://www.suse.com/security/cve/CVE-2019-25013/

https://www.suse.com/security/cve/CVE-2020-27618/

https://www.suse.com/security/cve/CVE-2020-29562/

https://www.suse.com/security/cve/CVE-2020-29573/

https://www.suse.com/security/cve/CVE-2021-3326/

http://www.nessus.org/u?538c9175

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-653=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-653=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-653=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-653=1

SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-653=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-653=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-653=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-653=1
SUSE Linux Enterprise Module for Development Tools 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Development-Tools-15-SP2-2021-653=1
SUSE Linux Enterprise Module for Basesystem 15-SP2 :
zypper in -t patch SUSE-SLE-Module-Basesystem-15-SP2-2021-653=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-653=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-653=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-653=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-653=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-653=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

High

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVSS v3.0 Temporal Score

5.2 (E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2019-25013
CVE	CVE-2020-29562
CVE	CVE-2020-29573
CVE	CVE-2021-3326
CVE	CVE-2020-27618

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/01, Modification date: 2021/03/03

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : glibc-2.26-13.51.1
Should be                : glibc-2.26-13.56.1
```

```
Remote package installed : glibc-extra-2.26-13.51.1
Should be                : glibc-extra-2.26-13.56.1

Remote package installed : glibc-locale-2.26-13.51.1
Should be                : glibc-locale-2.26-13.56.1

Remote package installed : glibc-locale-base-2.26-13.51.1
Should be                : glibc-locale-base-2.26-13.56.1

Remote package installed : nscd-2.26-13.51.1
Should be                : nscd-2.26-13.56.1
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

http://www.nessus.org/u?3a040ada

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/06/05, Modification date: 2021/03/09

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                         Code             KEX           Auth     Encryption
 MAC
   ----------------------       ----------       ---           ----     ---------------------
 ---
   DHE-RSA-AES128-SHA256        0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
   DHE-RSA-AES256-SHA384        0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
   ECDHE-RSA-AES128-SHA256      0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
   ECDHE-RSA-AES256-SHA384      0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
   DHE-RSA-AES128-SHA           0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
   DHE-RSA-AES256-SHA           0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
   ECDHE-RSA-AES128-SHA         0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
   ECDHE-RSA-AES256-SHA         0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
   DHE-RSA-AES128-SHA256        0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
   DHE-RSA-AES256-SHA256        0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
```

```
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH           RSA       AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH           RSA       AES-CBC(256)
SHA384


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX            Auth      Encryption
MAC
   ----------------------        ----------       ---            ----      --------------------
---
   DHE-RSA-AES128-SHA            0x00, 0x33       DH             RSA       AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH             [...]
```

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 do all requested local 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 allow all requested local checks.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVB:0001-B-0502

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2018/06/06, Modification date: 2021/04/12

Ports

172.16.4.38 (TCP/22) Vulnerability State: Active

```
Nessus was able to log in to the remote host via the following
protocol as iplroot, however this credential did not have
sufficient privileges for all planned checks :

  Protocol        : SSH
  Port            : 22

See the output of the following plugin for details :

  Plugin ID   : 102094
  Plugin Name : SSH Commands Require Privilege Escalation
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/12/15, Modification date: 2020/04/27

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=DE/O=SAP SE/OU=Connectivity/CN=SCC
|-Issuer  : C=DE/O=SAP SE/OU=Connectivity/CN=SCC
```

147571 - SUSE SLES15 Security Update : openssl-1_1 (SUSE-SU-2021:0753-1)

Synopsis

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

Description

This update for openssl-1_1 fixes the following issues :
CVE-2021-23840: Fixed an Integer overflow in CipherUpdate (bsc#1182333)
CVE-2021-23841: Fixed a NULL pointer dereference in X509_issuer_and_serial_hash() (bsc#1182331)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182333

https://www.suse.com/security/cve/CVE-2021-23840/

https://bugzilla.suse.com/show_bug.cgi?id=1182331

https://www.suse.com/security/cve/CVE-2021-23841/

http://www.nessus.org/u?12d34e0d

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-753=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-753=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-753=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-753=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-753=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-753=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-753=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-753=1
SUSE Enterprise Storage 6 :
zypper in -t patch SUSE-Storage-6-2021-753=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.1

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-23840
CVE	CVE-2021-23841

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/10, Modification date: 2021/03/12

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : libopenssl1_1-1.1.0i-14.12.1
Should be                : libopenssl1_1-1.1.0i-14.15.1

Remote package installed : openssl-1_1-1.1.0i-14.12.1
Should be                : openssl-1_1-1.1.0i-14.15.1
```

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.

See Also

Solution

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

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

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

 - ::1 (on interface lo)
 - fe80::20d:3aff:fe3e:46d8 (on interface eth0)
```

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).

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 100
```

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.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2005/08/26, Modification date: 2021/01/27

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 8.14.0
Plugin feed version : 202105011517
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Network Scan
Scanner IP : 10.10.112.28
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 62.502 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'iplroot' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/5/3 12:08 India Standard Time
Scan duration : 535 sec
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/05/04, Modification date: 2020/05/04

Ports

172.16.4.38 (TCP/8443) Vulnerability State: Resurfaced

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

147938 - SUSE SLES15 Security Update : glib2 (SUSE-SU-2021:0890-1)

Synopsis

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

Description

This update for glib2 fixes the following issues :
CVE-2021-27218: g_byte_array_new_take takes a gsize as length but stores in a guint, this patch will refuse if the length is larger than guint. (bsc#1182328)
CVE-2021-27219: g_memdup takes a guint as parameter and sometimes leads into an integer overflow, so add a g_memdup2 function which uses gsize to replace it. (bsc#1182362)
Note that Tenable Network Security has extracted the preceding description block directly from the SUSE security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://bugzilla.suse.com/show_bug.cgi?id=1182328

https://bugzilla.suse.com/show_bug.cgi?id=1182362

https://www.suse.com/security/cve/CVE-2021-27218/

https://www.suse.com/security/cve/CVE-2021-27219/

http://www.nessus.org/u?39302a36

Solution

To install this SUSE Security Update use the SUSE recommended installation methods like YaST online_update or 'zypper patch'.
Alternatively you can run the command listed for your product :
SUSE Manager Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Server-4.0-2021-890=1
SUSE Manager Retail Branch Server 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Retail-Branch-Server-4.0-2021-890=1
SUSE Manager Proxy 4.0 :
zypper in -t patch SUSE-SLE-Product-SUSE-Manager-Proxy-4.0-2021-890=1
SUSE Linux Enterprise Server for SAP 15-SP1 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-SP1-2021-890=1
SUSE Linux Enterprise Server for SAP 15 :
zypper in -t patch SUSE-SLE-Product-SLES_SAP-15-2021-890=1
SUSE Linux Enterprise Server 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-LTSS-2021-890=1
SUSE Linux Enterprise Server 15-SP1-BCL :
zypper in -t patch SUSE-SLE-Product-SLES-15-SP1-BCL-2021-890=1
SUSE Linux Enterprise Server 15-LTSS :
zypper in -t patch SUSE-SLE-Product-SLES-15-2021-890=1
SUSE Linux Enterprise High Performance Computing 15-SP1-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-LTSS-2021-890=1
SUSE Linux Enterprise High Performance Computing 15-SP1-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-SP1-ESPOS-2021-890=1
SUSE Linux Enterprise High Performance Computing 15-LTSS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-890=1
SUSE Linux Enterprise High Performance Computing 15-ESPOS :
zypper in -t patch SUSE-SLE-Product-HPC-15-2021-890=1
SUSE Enterprise Storage 6 :

zypper in -t patch SUSE-Storage-6-2021-890=1
SUSE CaaS Platform 4.0 :
To install this update, use the SUSE CaaS Platform 'skuba' tool. I will inform you if it detects new updates and let you then trigger updating of the complete cluster in a controlled way.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.1

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2021-27219
CVE	CVE-2021-27218

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2021/03/22, Modification date: 2021/03/24

Ports

172.16.4.38 (TCP/0) Vulnerability State: Active

```
Remote package installed : glib2-tools-2.54.3-4.21.1
Should be                : glib2-tools-2.54.3-4.24.1

Remote package installed : libgio-2_0-0-2.54.3-4.21.1
Should be                : libgio-2_0-0-2.54.3-4.24.1

Remote package installed : libglib-2_0-0-2.54.3-4.21.1
Should be                : libglib-2_0-0-2.54.3-4.24.1

Remote package installed : libgmodule-2_0-0-2.54.3-4.21.1
Should be                : libgmodule-2_0-0-2.54.3-4.24.1

Remote package installed : libgobject-2_0-0-2.54.3-4.21.1
Should be                : libgobject-2_0-0-2.54.3-4.24.1

Remote package installed : libgthread-2_0-0-2.54.3-4.21.1
Should be                : libgthread-2_0-0-2.54.3-4.24.1
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/11/27, Modification date: 2020/08/20

Ports

172.16.4.38 (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 10.10.112.28 to 172.16.4.38 :
10.10.112.28
10.10.112.1
10.10.96.101
10.77.81.165
10.6.225.245
10.6.225.246
?
172.16.4.38

Hop Count: 7
```