2019-MAR-06
FSL version 7.6.99

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

147690 - SuSE Linux 15.0 openSUSE-SU-2019:0252-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0252-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00149.html

SuSE Linux 15.0
x86_64
docker-runc-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.7.1
docker-runc-debuginfo-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.7.1

noarch
docker-runc-test-1.0.0rc5+gitr3562_69663f0bd4b6-lp150.5.7.1

194832 - Fedora Linux 29 FEDORA-2019-dfef0af227 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2004-2687

Description

The scan detected that the host is missing the following update:
FEDORA-2019-dfef0af227

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

distcc-3.2rc1-22.fc29

194833 - Fedora Linux 28 FEDORA-2019-a5f616808e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-5736, CVE-2019-8308

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a5f616808e

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 28

flatpak-1.0.7-1.fc28

194845 - Fedora Linux 29 FEDORA-2019-0a5e82cea8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-5704

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0a5e82cea8

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

openocd-0.10.0-11.fc29

194847 - Fedora Linux 28 FEDORA-2019-2c2dfc65d1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2004-2687

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2c2dfc65d1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

distcc-3.2rc1-22.fc28

24795 - Joomla Implement The TYPO3 PHAR Stream Wrapper Vulnerability (20190206)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: High

CVE: CVE-2019-7743

Description

A vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

A vulnerability is present in some versions of Joomla!. The flaw is due to the absence of protection mechanism in phar:// stream wrapper. Successful exploitation could allow an attacker to bypass certain security restrictions.

131304 - Debian Linux 9.0 DSA-4398-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024

Description

The scan detected that the host is missing the following update:
DSA-4398-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4398

Debian 9.0
all
php7.0_7.0.33-0+deb9u2

131307 - Debian Linux 9.0 DSA-4401-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-20147, CVE-2018-20148, CVE-2018-20149, CVE-2018-20150, CVE-2018-20151, CVE-2018-20152, CVE-2018-20153, CVE-2019-8942

Description

The scan detected that the host is missing the following update:
DSA-4401-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

http://www.debian.org/security/2019/dsa-4401

Debian 9.0
all
wordpress_4.7.5+dfsg-2+deb9u5

132497 - Oracle VM OVMSA-2019-0008 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2011-1485, CVE-2013-4288, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0008

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2019-March/000929.html
http://oss.oracle.com/pipermail/oraclevm-errata/2019-March/000930.html

OVM3.3
x86_64
polkit-0.96-11.el6_10.1

OVM3.4
x86_64
polkit-0.96-11.el6_10.1

147676 - SuSE Linux 42.3 openSUSE-SU-2019:0291-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0291-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00021.html

SuSE Linux 42.3
x86_64
procps-3.3.9-23.1
libprocps3-3.3.9-23.1
procps-devel-3.3.9-23.1
libprocps3-debuginfo-3.3.9-23.1
procps-debugsource-3.3.9-23.1

procps-debuginfo-3.3.9-23.1

i586
procps-3.3.9-23.1
libprocps3-3.3.9-23.1
procps-devel-3.3.9-23.1
libprocps3-debuginfo-3.3.9-23.1
procps-debugsource-3.3.9-23.1
procps-debuginfo-3.3.9-23.1

147677 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0541-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-1120, CVE-2018-16862, CVE-2018-16884, CVE-2018-19407, CVE-2018-19824, CVE-2018-19985, CVE-2018-20169, CVE-2018-5391, CVE-2018-9568, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0541-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005168.html
http://lists.suse.com/pipermail/sle-security-updates/2019-March/005167.html

SuSE SLED 12 SP3
x86_64
kernel-default-extra-4.4.175-94.79.1
kernel-default-devel-4.4.175-94.79.1
kernel-default-debugsource-4.4.175-94.79.1
kernel-default-extra-debuginfo-4.4.175-94.79.1
kernel-default-debuginfo-4.4.175-94.79.1
kernel-default-4.4.175-94.79.1
kernel-syms-4.4.175-94.79.1

noarch
kernel-macros-4.4.175-94.79.1
kernel-devel-4.4.175-94.79.1
kernel-source-4.4.175-94.79.1

SuSE SLES 12 SP3
noarch
kernel-macros-4.4.175-94.79.1
kernel-devel-4.4.175-94.79.1
kernel-source-4.4.175-94.79.1

x86_64
kernel-default-base-debuginfo-4.4.175-94.79.1
kernel-default-devel-4.4.175-94.79.1
kernel-default-debugsource-4.4.175-94.79.1
kernel-default-base-4.4.175-94.79.1
kernel-default-debuginfo-4.4.175-94.79.1
kernel-default-4.4.175-94.79.1
kernel-syms-4.4.175-94.79.1

147679 - SuSE Linux 15.0 openSUSE-SU-2019:0261-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-3827

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0261-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00151.html

SuSE Linux 15.0
i586
gvfs-fuse-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-devel-1.34.2.1-lp150.3.6.1
gvfs-backend-samba-1.34.2.1-lp150.3.6.1
gvfs-backends-1.34.2.1-lp150.3.6.1
gvfs-debugsource-1.34.2.1-lp150.3.6.1
gvfs-1.34.2.1-lp150.3.6.1
gvfs-backend-samba-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-backend-afc-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-backends-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-fuse-1.34.2.1-lp150.3.6.1
gvfs-backend-afc-1.34.2.1-lp150.3.6.1

noarch
gvfs-lang-1.34.2.1-lp150.3.6.1

x86_64
gvfs-backends-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-32bit-1.34.2.1-lp150.3.6.1
gvfs-debugsource-1.34.2.1-lp150.3.6.1
gvfs-backends-1.34.2.1-lp150.3.6.1
gvfs-1.34.2.1-lp150.3.6.1
gvfs-backend-samba-1.34.2.1-lp150.3.6.1
gvfs-backend-afc-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-backend-samba-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-fuse-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-devel-1.34.2.1-lp150.3.6.1
gvfs-32bit-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-debuginfo-1.34.2.1-lp150.3.6.1
gvfs-fuse-1.34.2.1-lp150.3.6.1
gvfs-backend-afc-1.34.2.1-lp150.3.6.1

147680 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0512-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0512-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005163.html

SuSE SLED 12 SP4
x86_64
libopenssl1_1-debuginfo-32bit-1.1.1-2.6.1
libopenssl1_1-debuginfo-1.1.1-2.6.1
openssl-1_1-debugsource-1.1.1-2.6.1
openssl-1_1-debuginfo-1.1.1-2.6.1
libopenssl1_1-1.1.1-2.6.1
libopenssl1_1-32bit-1.1.1-2.6.1

SuSE SLES 12 SP4
x86_64
libopenssl1_1-debuginfo-32bit-1.1.1-2.6.1
libopenssl1_1-debuginfo-1.1.1-2.6.1
openssl-1_1-debugsource-1.1.1-2.6.1
openssl-1_1-debuginfo-1.1.1-2.6.1
libopenssl1_1-1.1.1-2.6.1
libopenssl1_1-32bit-1.1.1-2.6.1

147682 - SuSE SLED 15 SUSE-SU-2019:0539-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-0886, CVE-2018-1000852, CVE-2018-8784, CVE-2018-8785, CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0539-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-March/005170.html

SuSE SLED 15
x86_64
libfreerdp2-debuginfo-2.0.0~rc4-3.3.1
freerdp-debuginfo-2.0.0~rc4-3.3.1
freerdp-2.0.0~rc4-3.3.1
freerdp-debugsource-2.0.0~rc4-3.3.1
libfreerdp2-2.0.0~rc4-3.3.1
freerdp-devel-2.0.0~rc4-3.3.1
libwinpr2-2.0.0~rc4-3.3.1
winpr2-devel-2.0.0~rc4-3.3.1
libwinpr2-debuginfo-2.0.0~rc4-3.3.1

147683 - SuSE Linux 15.0 openSUSE-SU-2019:0265-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-15518, CVE-2018-19873

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0265-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00157.html

SuSE Linux 15.0
i586
libQt5Core5-5.9.4-lp150.5.4.1
libQt5Test5-debuginfo-5.9.4-lp150.5.4.1
libQt5Network-devel-5.9.4-lp150.5.4.1
libQt5DBus-devel-5.9.4-lp150.5.4.1
libQt5Sql5-postgresql-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-5.9.4-lp150.5.4.1
libQt5PrintSupport5-debuginfo-5.9.4-lp150.5.4.1
libQt5OpenGLExtensions-devel-static-5.9.4-lp150.5.4.1
libQt5DBus5-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-debuginfo-5.9.4-lp150.5.4.1
libQt5PlatformSupport-devel-static-5.9.4-lp150.5.4.1
libQt5KmsSupport-devel-static-5.9.4-lp150.5.4.1
libQt5Concurrent-devel-5.9.4-lp150.5.4.1
libQt5OpenGL-devel-5.9.4-lp150.5.4.1
libQt5Widgets5-5.9.4-lp150.5.4.1
libQt5Gui5-5.9.4-lp150.5.4.1
libQt5Concurrent5-debuginfo-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-5.9.4-lp150.5.4.1
libQt5Sql5-unixODBC-5.9.4-lp150.5.4.1
libQt5OpenGL5-5.9.4-lp150.5.4.1
libQt5Gui5-debuginfo-5.9.4-lp150.5.4.1
libQt5Concurrent5-5.9.4-lp150.5.4.1
libqt5-qtbase-debugsource-5.9.4-lp150.5.4.1
libQt5Network5-5.9.4-lp150.5.4.1
libQt5Test5-5.9.4-lp150.5.4.1
libQt5Sql5-postgresql-debuginfo-5.9.4-lp150.5.4.1
libQt5Core5-debuginfo-5.9.4-lp150.5.4.1
libQt5Widgets-devel-5.9.4-lp150.5.4.1
libQt5Core-devel-5.9.4-lp150.5.4.1
libqt5-qtbase-common-devel-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql-devel-5.9.4-lp150.5.4.1
libQt5Widgets5-debuginfo-5.9.4-lp150.5.4.1
libQt5OpenGL5-debuginfo-5.9.4-lp150.5.4.1
libQt5PlatformHeaders-devel-5.9.4-lp150.5.4.1
libqt5-qtbase-common-devel-5.9.4-lp150.5.4.1
libqt5-qtbase-platformtheme-gtk3-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-debuginfo-5.9.4-lp150.5.4.1
libQt5Xml5-5.9.4-lp150.5.4.1
libQt5DBus-devel-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-debuginfo-5.9.4-lp150.5.4.1
libQt5Xml-devel-5.9.4-lp150.5.4.1

libQt5Sql5-unixODBC-debuginfo-5.9.4-lp150.5.4.1
libQt5Bootstrap-devel-static-5.9.4-lp150.5.4.1
libQt5Network5-debuginfo-5.9.4-lp150.5.4.1
libqt5-qtbase-platformtheme-gtk3-5.9.4-lp150.5.4.1
libQt5DBus5-debuginfo-5.9.4-lp150.5.4.1
libQt5Test-devel-5.9.4-lp150.5.4.1
libQt5PrintSupport5-5.9.4-lp150.5.4.1
libQt5Sql5-5.9.4-lp150.5.4.1
libqt5-qtbase-devel-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-5.9.4-lp150.5.4.1
libQt5Gui-devel-5.9.4-lp150.5.4.1
libQt5PrintSupport-devel-5.9.4-lp150.5.4.1
libQt5Xml5-debuginfo-5.9.4-lp150.5.4.1

noarch
libqt5-qtbase-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Test-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Sql-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Gui-private-headers-devel-5.9.4-lp150.5.4.1
libQt5PlatformSupport-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Core-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Network-private-headers-devel-5.9.4-lp150.5.4.1
libQt5PrintSupport-private-headers-devel-5.9.4-lp150.5.4.1
libQt5KmsSupport-private-headers-devel-5.9.4-lp150.5.4.1
libQt5OpenGL-private-headers-devel-5.9.4-lp150.5.4.1
libQt5DBus-private-headers-devel-5.9.4-lp150.5.4.1
libQt5Widgets-private-headers-devel-5.9.4-lp150.5.4.1

x86_64
libQt5PrintSupport5-debuginfo-5.9.4-lp150.5.4.1
libQt5DBus5-32bit-5.9.4-lp150.5.4.1
libQt5Concurrent-devel-32bit-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-32bit-5.9.4-lp150.5.4.1
libQt5Test5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-unixODBC-5.9.4-lp150.5.4.1
libQt5PlatformSupport-devel-static-32bit-5.9.4-lp150.5.4.1
libqt5-qtbase-platformtheme-gtk3-debuginfo-5.9.4-lp150.5.4.1
libQt5Xml-devel-32bit-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-32bit-5.9.4-lp150.5.4.1
libQt5OpenGL5-32bit-5.9.4-lp150.5.4.1
libQt5Xml5-debuginfo-5.9.4-lp150.5.4.1
libQt5Core5-32bit-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-debuginfo-5.9.4-lp150.5.4.1
libqt5-qtbase-devel-5.9.4-lp150.5.4.1
libQt5Sql5-unixODBC-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-unixODBC-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Concurrent5-debuginfo-5.9.4-lp150.5.4.1
libQt5Concurrent5-32bit-5.9.4-lp150.5.4.1
libQt5Gui5-32bit-5.9.4-lp150.5.4.1
libQt5Network5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5DBus-devel-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Core5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Widgets-devel-32bit-5.9.4-lp150.5.4.1
libQt5PrintSupport5-32bit-5.9.4-lp150.5.4.1
libQt5Test5-32bit-5.9.4-lp150.5.4.1
libQt5Sql5-5.9.4-lp150.5.4.1
libQt5Widgets5-32bit-5.9.4-lp150.5.4.1
libQt5Sql-devel-32bit-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-debuginfo-5.9.4-lp150.5.4.1

libQt5Test5-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Xml5-5.9.4-lp150.5.4.1
libQt5Network5-debuginfo-5.9.4-lp150.5.4.1
libQt5OpenGLExtensions-devel-static-5.9.4-lp150.5.4.1
libQt5Concurrent5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-unixODBC-32bit-5.9.4-lp150.5.4.1
libQt5Concurrent5-5.9.4-lp150.5.4.1
libQt5PlatformSupport-devel-static-5.9.4-lp150.5.4.1
libQt5Network5-5.9.4-lp150.5.4.1
libQt5PrintSupport-devel-32bit-5.9.4-lp150.5.4.1
libQt5Bootstrap-devel-static-5.9.4-lp150.5.4.1
libQt5DBus5-5.9.4-lp150.5.4.1
libQt5Sql5-postgresql-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-5.9.4-lp150.5.4.1
libQt5Xml5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Gui5-32bit-debuginfo-5.9.4-lp150.5.4.1
libqt5-qtbase-debugsource-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Core5-debuginfo-5.9.4-lp150.5.4.1
libQt5PrintSupport5-5.9.4-lp150.5.4.1
libqt5-qtbase-examples-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-32bit-5.9.4-lp150.5.4.1
libQt5Gui5-5.9.4-lp150.5.4.1
libQt5Widgets5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Test-devel-32bit-5.9.4-lp150.5.4.1
libQt5Gui5-debuginfo-5.9.4-lp150.5.4.1
libQt5OpenGL5-5.9.4-lp150.5.4.1
libQt5Test5-debuginfo-5.9.4-lp150.5.4.1
libQt5PrintSupport-devel-5.9.4-lp150.5.4.1
libQt5Sql5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Widgets5-5.9.4-lp150.5.4.1
libQt5Gui-devel-5.9.4-lp150.5.4.1
libQt5OpenGL5-debuginfo-5.9.4-lp150.5.4.1
libQt5PrintSupport5-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5DBus5-debuginfo-5.9.4-lp150.5.4.1
libQt5Bootstrap-devel-static-32bit-5.9.4-lp150.5.4.1
libQt5Sql-devel-5.9.4-lp150.5.4.1
libQt5KmsSupport-devel-static-5.9.4-lp150.5.4.1
libQt5PlatformHeaders-devel-5.9.4-lp150.5.4.1
libQt5Gui-devel-32bit-5.9.4-lp150.5.4.1
libQt5DBus-devel-32bit-5.9.4-lp150.5.4.1
libQt5OpenGL-devel-5.9.4-lp150.5.4.1
libQt5Core-devel-32bit-5.9.4-lp150.5.4.1
libQt5Xml5-32bit-5.9.4-lp150.5.4.1
libQt5OpenGL5-32bit-debuginfo-5.9.4-lp150.5.4.1
libqt5-qtbase-common-devel-5.9.4-lp150.5.4.1
libQt5DBus-devel-debuginfo-5.9.4-lp150.5.4.1
libQt5Widgets5-debuginfo-5.9.4-lp150.5.4.1
libQt5Xml-devel-5.9.4-lp150.5.4.1
libQt5Core-devel-5.9.4-lp150.5.4.1
libQt5Sql5-sqlite-5.9.4-lp150.5.4.1
libQt5Sql5-postgresql-32bit-debuginfo-5.9.4-lp150.5.4.1
libQt5Sql5-mysql-debuginfo-5.9.4-lp150.5.4.1
libQt5Network-devel-5.9.4-lp150.5.4.1
libQt5Sql5-32bit-5.9.4-lp150.5.4.1
libQt5Widgets-devel-5.9.4-lp150.5.4.1
libQt5DBus-devel-5.9.4-lp150.5.4.1
libQt5Sql5-debuginfo-5.9.4-lp150.5.4.1
libQt5Network5-32bit-5.9.4-lp150.5.4.1

libqt5-qtbase-common-devel-debuginfo-5.9.4-lp150.5.4.1
libQt5Network-devel-32bit-5.9.4-lp150.5.4.1

147685 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0511-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-6212, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226, CVE-2019-6227, CVE-2019-6229, CVE-2019-6233, CVE-2019-6234

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0511-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005162.html

SuSE SLES 12 SP3
x86_64
typelib-1_0-WebKit2-4_0-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-2.35.1
webkit2gtk3-debugsource-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-2.22.6-2.35.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-2.35.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-2.35.1
libwebkit2gtk-4_0-37-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-2.22.6-2.35.1

SuSE SLES 12 SP4
x86_64
typelib-1_0-WebKit2-4_0-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-2.35.1
webkit2gtk3-debugsource-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-2.22.6-2.35.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-2.35.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-2.35.1
libwebkit2gtk-4_0-37-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-2.22.6-2.35.1

SuSE SLED 12 SP4
x86_64
typelib-1_0-WebKit2-4_0-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-2.35.1
webkit2gtk3-debugsource-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-2.22.6-2.35.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-2.35.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-2.35.1
libwebkit2gtk-4_0-37-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-2.22.6-2.35.1

noarch
libwebkit2gtk3-lang-2.22.6-2.35.1

SuSE SLED 12 SP3
x86_64
typelib-1_0-WebKit2-4_0-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.6-2.35.1
webkit2gtk3-debugsource-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-2.22.6-2.35.1
libwebkit2gtk-4_0-37-debuginfo-2.22.6-2.35.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.6-2.35.1
typelib-1_0-JavaScriptCore-4_0-2.22.6-2.35.1
libwebkit2gtk-4_0-37-2.22.6-2.35.1
libjavascriptcoregtk-4_0-18-2.22.6-2.35.1

noarch
libwebkit2gtk3-lang-2.22.6-2.35.1

147688 - SuSE Linux 15.0 openSUSE-SU-2019:0251-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-12405, CVE-2018-17466, CVE-2018-18335, CVE-2018-18356, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505, CVE-2018-18509, CVE-2019-5785

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0251-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00145.html

SuSE Linux 15.0
x86_64
MozillaThunderbird-debugsource-60.5.1-lp150.3.30.1
MozillaThunderbird-translations-common-60.5.1-lp150.3.30.1
MozillaThunderbird-debuginfo-60.5.1-lp150.3.30.1
MozillaThunderbird-60.5.1-lp150.3.30.1
MozillaThunderbird-translations-other-60.5.1-lp150.3.30.1
MozillaThunderbird-buildsymbols-60.5.1-lp150.3.30.1

147689 - SuSE Linux 15.0 openSUSE-SU-2019:0293-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-19637, CVE-2018-19638, CVE-2018-19639, CVE-2018-19640

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0293-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00023.html

SuSE Linux 15.0
noarch
supportutils-3.1-lp150.4.3.1

147691 - SuSE Linux 42.3 openSUSE-SU-2019:0274-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0274-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00001.html

SuSE Linux 42.3
x86_64
kernel-debug-base-4.4.175-89.1
kernel-default-base-debuginfo-4.4.175-89.1
kernel-default-base-4.4.175-89.1
kernel-debug-devel-4.4.175-89.1
kernel-debug-debuginfo-4.4.175-89.1
kernel-syms-4.4.175-89.1
kernel-default-4.4.175-89.1
kernel-default-debugsource-4.4.175-89.1
kernel-default-devel-4.4.175-89.1
kernel-obs-build-debugsource-4.4.175-89.1
kernel-obs-build-4.4.175-89.1
kernel-vanilla-debuginfo-4.4.175-89.1
kernel-default-debuginfo-4.4.175-89.1
kernel-debug-base-debuginfo-4.4.175-89.1
kernel-debug-4.4.175-89.1
kernel-obs-qa-4.4.175-89.1
kernel-vanilla-base-4.4.175-89.1
kernel-vanilla-base-debuginfo-4.4.175-89.1
kernel-vanilla-debugsource-4.4.175-89.1
kernel-debug-devel-debuginfo-4.4.175-89.1
kernel-debug-debugsource-4.4.175-89.1
kernel-vanilla-devel-4.4.175-89.1
kernel-vanilla-4.4.175-89.1

noarch
kernel-docs-pdf-4.4.175-89.1
kernel-docs-4.4.175-89.1
kernel-source-vanilla-4.4.175-89.1
kernel-docs-html-4.4.175-89.1
kernel-source-4.4.175-89.1
kernel-macros-4.4.175-89.1
kernel-devel-4.4.175-89.1

147692 - SuSE Linux 15.0 openSUSE-SU-2019:0255-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0255-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00148.html

SuSE Linux 15.0
i586
libudev-mini-devel-234-lp150.20.15.1
systemd-mini-debugsource-234-lp150.20.15.1
systemd-mini-container-mini-234-lp150.20.15.1
systemd-234-lp150.20.15.1
nss-myhostname-234-lp150.20.15.1
libudev1-234-lp150.20.15.1
systemd-sysvinit-234-lp150.20.15.1
systemd-devel-234-lp150.20.15.1
libsystemd0-234-lp150.20.15.1
systemd-mini-234-lp150.20.15.1
libsystemd0-debuginfo-234-lp150.20.15.1
systemd-container-234-lp150.20.15.1
systemd-coredump-debuginfo-234-lp150.20.15.1
systemd-debuginfo-234-lp150.20.15.1
systemd-mini-sysvinit-234-lp150.20.15.1
nss-myhostname-debuginfo-234-lp150.20.15.1
udev-mini-debuginfo-234-lp150.20.15.1
nss-systemd-234-lp150.20.15.1
systemd-debugsource-234-lp150.20.15.1
nss-mymachines-debuginfo-234-lp150.20.15.1
systemd-logger-234-lp150.20.15.1
systemd-mini-container-mini-debuginfo-234-lp150.20.15.1
libsystemd0-mini-debuginfo-234-lp150.20.15.1
udev-debuginfo-234-lp150.20.15.1
systemd-mini-devel-234-lp150.20.15.1
udev-234-lp150.20.15.1
libudev1-debuginfo-234-lp150.20.15.1
nss-mymachines-234-lp150.20.15.1
nss-systemd-debuginfo-234-lp150.20.15.1
udev-mini-234-lp150.20.15.1
systemd-mini-coredump-mini-234-lp150.20.15.1
libsystemd0-mini-234-lp150.20.15.1
systemd-mini-coredump-mini-debuginfo-234-lp150.20.15.1
systemd-container-debuginfo-234-lp150.20.15.1
systemd-mini-debuginfo-234-lp150.20.15.1
libudev-devel-234-lp150.20.15.1
libudev-mini1-debuginfo-234-lp150.20.15.1
systemd-coredump-234-lp150.20.15.1
libudev-mini1-234-lp150.20.15.1

noarch

systemd-bash-completion-234-lp150.20.15.1
systemd-mini-bash-completion-234-lp150.20.15.1

x86_64
systemd-32bit-234-lp150.20.15.1
libudev-mini-devel-234-lp150.20.15.1
systemd-mini-debugsource-234-lp150.20.15.1
libsystemd0-32bit-debuginfo-234-lp150.20.15.1
systemd-mini-container-mini-234-lp150.20.15.1
systemd-234-lp150.20.15.1
libsystemd0-32bit-234-lp150.20.15.1
nss-mymachines-32bit-debuginfo-234-lp150.20.15.1
nss-myhostname-234-lp150.20.15.1
libudev1-234-lp150.20.15.1
systemd-sysvinit-234-lp150.20.15.1
systemd-devel-234-lp150.20.15.1
systemd-32bit-debuginfo-234-lp150.20.15.1
libsystemd0-234-lp150.20.15.1
systemd-mini-234-lp150.20.15.1
nss-myhostname-32bit-234-lp150.20.15.1
nss-mymachines-32bit-234-lp150.20.15.1
libudev1-32bit-234-lp150.20.15.1
libsystemd0-debuginfo-234-lp150.20.15.1
systemd-container-234-lp150.20.15.1
systemd-coredump-debuginfo-234-lp150.20.15.1
systemd-debuginfo-234-lp150.20.15.1
systemd-mini-sysvinit-234-lp150.20.15.1
nss-myhostname-debuginfo-234-lp150.20.15.1
udev-mini-debuginfo-234-lp150.20.15.1
nss-systemd-234-lp150.20.15.1
systemd-debugsource-234-lp150.20.15.1
nss-mymachines-debuginfo-234-lp150.20.15.1
systemd-logger-234-lp150.20.15.1
systemd-mini-container-mini-debuginfo-234-lp150.20.15.1
libsystemd0-mini-debuginfo-234-lp150.20.15.1
udev-debuginfo-234-lp150.20.15.1
systemd-mini-devel-234-lp150.20.15.1
nss-myhostname-32bit-debuginfo-234-lp150.20.15.1
udev-234-lp150.20.15.1
libudev1-debuginfo-234-lp150.20.15.1
nss-mymachines-234-lp150.20.15.1
nss-systemd-debuginfo-234-lp150.20.15.1
libudev-devel-32bit-234-lp150.20.15.1
udev-mini-234-lp150.20.15.1
systemd-mini-coredump-mini-234-lp150.20.15.1
libsystemd0-mini-234-lp150.20.15.1
systemd-mini-coredump-mini-debuginfo-234-lp150.20.15.1
systemd-container-debuginfo-234-lp150.20.15.1
systemd-mini-debuginfo-234-lp150.20.15.1
libudev-devel-234-lp150.20.15.1
libudev-mini1-debuginfo-234-lp150.20.15.1
systemd-coredump-234-lp150.20.15.1
libudev-mini1-234-lp150.20.15.1
libudev1-32bit-debuginfo-234-lp150.20.15.1

147693 - SuSE Linux 42.3 openSUSE-SU-2019:0268-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-6454

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0268-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00160.html

SuSE Linux 42.3
i586
libudev-mini1-228-68.1
nss-mymachines-debuginfo-228-68.1
systemd-debugsource-228-68.1
systemd-228-68.1
systemd-logger-228-68.1
systemd-debuginfo-228-68.1
udev-debuginfo-228-68.1
nss-myhostname-228-68.1
systemd-mini-debuginfo-228-68.1
systemd-sysvinit-228-68.1
systemd-mini-devel-228-68.1
udev-mini-debuginfo-228-68.1
libsystemd0-debuginfo-228-68.1
udev-mini-228-68.1
libsystemd0-228-68.1
libudev-mini-devel-228-68.1
libsystemd0-mini-228-68.1
systemd-mini-sysvinit-228-68.1
systemd-mini-debugsource-228-68.1
systemd-devel-228-68.1
libudev-devel-228-68.1
libudev1-228-68.1
udev-228-68.1
libudev1-debuginfo-228-68.1
libudev-mini1-debuginfo-228-68.1
libsystemd0-mini-debuginfo-228-68.1
systemd-mini-228-68.1
nss-myhostname-debuginfo-228-68.1
nss-mymachines-228-68.1

noarch
systemd-bash-completion-228-68.1
systemd-mini-bash-completion-228-68.1

x86_64
libudev1-debuginfo-32bit-228-68.1
libudev-mini1-228-68.1
nss-mymachines-debuginfo-228-68.1
systemd-debugsource-228-68.1
systemd-228-68.1
systemd-logger-228-68.1
systemd-debuginfo-228-68.1
udev-debuginfo-228-68.1
nss-myhostname-228-68.1
systemd-mini-debuginfo-228-68.1

systemd-32bit-228-68.1
systemd-sysvinit-228-68.1
systemd-mini-devel-228-68.1
udev-mini-debuginfo-228-68.1
libsystemd0-debuginfo-228-68.1
udev-mini-228-68.1
libsystemd0-228-68.1
libudev-mini-devel-228-68.1
libsystemd0-mini-228-68.1
systemd-mini-sysvinit-228-68.1
systemd-mini-debugsource-228-68.1
nss-myhostname-32bit-228-68.1
systemd-devel-228-68.1
libudev-devel-228-68.1
libudev1-228-68.1
libudev1-32bit-228-68.1
libsystemd0-debuginfo-32bit-228-68.1
udev-228-68.1
nss-myhostname-debuginfo-32bit-228-68.1
libudev1-debuginfo-228-68.1
libsystemd0-32bit-228-68.1
libudev-mini1-debuginfo-228-68.1
libsystemd0-mini-debuginfo-228-68.1
systemd-mini-228-68.1
nss-myhostname-debuginfo-228-68.1
systemd-debuginfo-32bit-228-68.1
nss-mymachines-228-68.1

186592 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3900-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-6977, CVE-2019-6978

Description

The scan detected that the host is missing the following update:
USN-3900-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004787.html

Ubuntu 16.04

libgd-tools_2.1.1-4ubuntu0.16.04.11
libgd3_2.1.1-4ubuntu0.16.04.11

Ubuntu 18.10

libgd-tools_2.2.5-4ubuntu1.1
libgd3_2.2.5-4ubuntu1.1

Ubuntu 14.04

libgd3_2.1.0-3ubuntu0.11
libgd-tools_2.1.0-3ubuntu0.11

Ubuntu 18.04

libgd3_2.2.5-4ubuntu0.3
libgd-tools_2.2.5-4ubuntu0.3

194834 - Fedora Linux 28 FEDORA-2019-02e13cb1a8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-20030

Description

The scan detected that the host is missing the following update:
FEDORA-2019-02e13cb1a8

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 28

libexif-0.6.21-19.fc28

194838 - Fedora Linux 29 FEDORA-2019-e3b2885a25 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-1000852, CVE-2018-8786

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e3b2885a25

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

gnome-boxes-3.30.3-2.fc29
pidgin-sipe-1.24.0-3.fc29
remmina-1.3.3-1.fc29
freerdp-2.0.0-48.20190228gitce386c8.fc29

194840 - Fedora Linux 28 FEDORA-2019-c54511eaab Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-10855, CVE-2018-10874, CVE-2018-10875, CVE-2019-3828

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c54511eaab

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

ansible-2.7.8-1.fc28

194846 - Fedora Linux 29 FEDORA-2019-7462acf8ba Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-16862, CVE-2018-16880, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9162

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7462acf8ba

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 29

kernel-headers-4.20.12-200.fc29
kernel-4.20.12-200.fc29

89008 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-060-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2016-9844, CVE-2018-1000035, CVE-2018-18384

Description

The scan detected that the host is missing the following update:
SSA:2019-060-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.453326

Slackware 14.0
x86_64
infozip-6.0-x86_64-2

Slackware 14.2
x86_64
infozip-6.0-x86_64-4

i586
infozip-6.0-i586-4

Slackware 14.1
x86_64
infozip-6.0-x86_64-4

147684 - SuSE Linux 15.0 openSUSE-SU-2019:0294-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-8358

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0294-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00022.html

SuSE Linux 15.0
x86_64
hiawatha-letsencrypt-10.8.4-lp150.2.4.1
hiawatha-10.8.4-lp150.2.4.1
hiawatha-debuginfo-10.8.4-lp150.2.4.1
hiawatha-debugsource-10.8.4-lp150.2.4.1

147687 - SuSE Linux 42.3 openSUSE-SU-2019:0276-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6977

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0276-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00007.html

SuSE Linux 42.3
i586
php5-json-debuginfo-5.5.14-112.1
apache2-mod_php5-debuginfo-5.5.14-112.1
php5-ctype-debuginfo-5.5.14-112.1

php5-enchant-debuginfo-5.5.14-112.1
php5-bz2-5.5.14-112.1
php5-xmlreader-debuginfo-5.5.14-112.1
php5-snmp-5.5.14-112.1
php5-sysvshm-5.5.14-112.1
php5-intl-5.5.14-112.1
php5-opcache-5.5.14-112.1
php5-phar-debuginfo-5.5.14-112.1
php5-fastcgi-debuginfo-5.5.14-112.1
php5-exif-debuginfo-5.5.14-112.1
php5-fpm-5.5.14-112.1
php5-xmlrpc-5.5.14-112.1
php5-devel-5.5.14-112.1
php5-pgsql-5.5.14-112.1
php5-zip-5.5.14-112.1
php5-fastcgi-5.5.14-112.1
php5-soap-5.5.14-112.1
php5-iconv-5.5.14-112.1
php5-imap-debuginfo-5.5.14-112.1
php5-fileinfo-debuginfo-5.5.14-112.1
php5-mysql-debuginfo-5.5.14-112.1
php5-mssql-5.5.14-112.1
php5-xmlreader-5.5.14-112.1
php5-pspell-5.5.14-112.1
php5-firebird-5.5.14-112.1
php5-mcrypt-debuginfo-5.5.14-112.1
php5-pspell-debuginfo-5.5.14-112.1
php5-firebird-debuginfo-5.5.14-112.1
php5-shmop-debuginfo-5.5.14-112.1
php5-shmop-5.5.14-112.1
php5-openssl-debuginfo-5.5.14-112.1
php5-tidy-5.5.14-112.1
php5-curl-5.5.14-112.1
php5-xsl-5.5.14-112.1
php5-enchant-5.5.14-112.1
php5-xsl-debuginfo-5.5.14-112.1
php5-dom-5.5.14-112.1
php5-bcmath-debuginfo-5.5.14-112.1
php5-dba-5.5.14-112.1
php5-debugsource-5.5.14-112.1
php5-5.5.14-112.1
php5-sysvsem-5.5.14-112.1
php5-mbstring-5.5.14-112.1
php5-json-5.5.14-112.1
php5-tokenizer-debuginfo-5.5.14-112.1
php5-tokenizer-5.5.14-112.1
php5-pdo-5.5.14-112.1
php5-gd-5.5.14-112.1
php5-readline-5.5.14-112.1
php5-pcntl-5.5.14-112.1
php5-sockets-5.5.14-112.1
php5-snmp-debuginfo-5.5.14-112.1
php5-mcrypt-5.5.14-112.1
php5-xmlwriter-5.5.14-112.1
php5-tidy-debuginfo-5.5.14-112.1
php5-zlib-5.5.14-112.1
php5-mbstring-debuginfo-5.5.14-112.1
php5-suhosin-5.5.14-112.1
php5-soap-debuginfo-5.5.14-112.1
php5-fpm-debuginfo-5.5.14-112.1

php5-posix-5.5.14-112.1
php5-sqlite-debuginfo-5.5.14-112.1
php5-exif-5.5.14-112.1
php5-gettext-debuginfo-5.5.14-112.1
php5-sockets-debuginfo-5.5.14-112.1
php5-gmp-debuginfo-5.5.14-112.1
php5-calendar-debuginfo-5.5.14-112.1
php5-zlib-debuginfo-5.5.14-112.1
php5-debuginfo-5.5.14-112.1
php5-wddx-5.5.14-112.1
php5-xmlrpc-debuginfo-5.5.14-112.1
php5-pdo-debuginfo-5.5.14-112.1
php5-zip-debuginfo-5.5.14-112.1
php5-mysql-5.5.14-112.1
php5-curl-debuginfo-5.5.14-112.1
php5-bcmath-5.5.14-112.1
php5-sysvshm-debuginfo-5.5.14-112.1
php5-phar-5.5.14-112.1
php5-wddx-debuginfo-5.5.14-112.1
php5-bz2-debuginfo-5.5.14-112.1
php5-posix-debuginfo-5.5.14-112.1
php5-ldap-5.5.14-112.1
php5-gd-debuginfo-5.5.14-112.1
php5-opcache-debuginfo-5.5.14-112.1
php5-iconv-debuginfo-5.5.14-112.1
php5-xmlwriter-debuginfo-5.5.14-112.1
php5-odbc-debuginfo-5.5.14-112.1
php5-intl-debuginfo-5.5.14-112.1
php5-imap-5.5.14-112.1
php5-odbc-5.5.14-112.1
apache2-mod_php5-5.5.14-112.1
php5-pgsql-debuginfo-5.5.14-112.1
php5-suhosin-debuginfo-5.5.14-112.1
php5-ldap-debuginfo-5.5.14-112.1
php5-gettext-5.5.14-112.1
php5-sysvsem-debuginfo-5.5.14-112.1
php5-gmp-5.5.14-112.1
php5-fileinfo-5.5.14-112.1
php5-readline-debuginfo-5.5.14-112.1
php5-sqlite-5.5.14-112.1
php5-ftp-debuginfo-5.5.14-112.1
php5-dba-debuginfo-5.5.14-112.1
php5-openssl-5.5.14-112.1
php5-dom-debuginfo-5.5.14-112.1
php5-ftp-5.5.14-112.1
php5-sysvmsg-5.5.14-112.1
php5-sysvmsg-debuginfo-5.5.14-112.1
php5-calendar-5.5.14-112.1
php5-mssql-debuginfo-5.5.14-112.1
php5-ctype-5.5.14-112.1
php5-pcntl-debuginfo-5.5.14-112.1

noarch
php5-pear-5.5.14-112.1

x86_64
php5-json-debuginfo-5.5.14-112.1
apache2-mod_php5-debuginfo-5.5.14-112.1
php5-ctype-debuginfo-5.5.14-112.1
php5-enchant-debuginfo-5.5.14-112.1

php5-bz2-5.5.14-112.1
php5-xmlreader-debuginfo-5.5.14-112.1
php5-snmp-5.5.14-112.1
php5-sysvshm-5.5.14-112.1
php5-intl-5.5.14-112.1
php5-opcache-5.5.14-112.1
php5-phar-debuginfo-5.5.14-112.1
php5-fastcgi-debuginfo-5.5.14-112.1
php5-exif-debuginfo-5.5.14-112.1
php5-fpm-5.5.14-112.1
php5-xmlrpc-5.5.14-112.1
php5-devel-5.5.14-112.1
php5-pgsql-5.5.14-112.1
php5-zip-5.5.14-112.1
php5-fastcgi-5.5.14-112.1
php5-soap-5.5.14-112.1
php5-iconv-5.5.14-112.1
php5-imap-debuginfo-5.5.14-112.1
php5-fileinfo-debuginfo-5.5.14-112.1
php5-mysql-debuginfo-5.5.14-112.1
php5-mssql-5.5.14-112.1
php5-xmlreader-5.5.14-112.1
php5-pspell-5.5.14-112.1
php5-firebird-5.5.14-112.1
php5-mcrypt-debuginfo-5.5.14-112.1
php5-pspell-debuginfo-5.5.14-112.1
php5-firebird-debuginfo-5.5.14-112.1
php5-shmop-debuginfo-5.5.14-112.1
php5-shmop-5.5.14-112.1
php5-openssl-debuginfo-5.5.14-112.1
php5-tidy-5.5.14-112.1
php5-curl-5.5.14-112.1
php5-xsl-5.5.14-112.1
php5-enchant-5.5.14-112.1
php5-xsl-debuginfo-5.5.14-112.1
php5-dom-5.5.14-112.1
php5-bcmath-debuginfo-5.5.14-112.1
php5-dba-5.5.14-112.1
php5-debugsource-5.5.14-112.1
php5-5.5.14-112.1
php5-sysvsem-5.5.14-112.1
php5-mbstring-5.5.14-112.1
php5-json-5.5.14-112.1
php5-tokenizer-debuginfo-5.5.14-112.1
php5-tokenizer-5.5.14-112.1
php5-pdo-5.5.14-112.1
php5-gd-5.5.14-112.1
php5-readline-5.5.14-112.1
php5-pcntl-5.5.14-112.1
php5-sockets-5.5.14-112.1
php5-snmp-debuginfo-5.5.14-112.1
php5-mcrypt-5.5.14-112.1
php5-xmlwriter-5.5.14-112.1
php5-tidy-debuginfo-5.5.14-112.1
php5-zlib-5.5.14-112.1
php5-mbstring-debuginfo-5.5.14-112.1
php5-suhosin-5.5.14-112.1
php5-soap-debuginfo-5.5.14-112.1
php5-fpm-debuginfo-5.5.14-112.1
php5-posix-5.5.14-112.1

php5-sqlite-debuginfo-5.5.14-112.1
php5-exif-5.5.14-112.1
php5-gettext-debuginfo-5.5.14-112.1
php5-sockets-debuginfo-5.5.14-112.1
php5-gmp-debuginfo-5.5.14-112.1
php5-calendar-debuginfo-5.5.14-112.1
php5-zlib-debuginfo-5.5.14-112.1
php5-debuginfo-5.5.14-112.1
php5-wddx-5.5.14-112.1
php5-xmlrpc-debuginfo-5.5.14-112.1
php5-pdo-debuginfo-5.5.14-112.1
php5-zip-debuginfo-5.5.14-112.1
php5-mysql-5.5.14-112.1
php5-curl-debuginfo-5.5.14-112.1
php5-bcmath-5.5.14-112.1
php5-sysvshm-debuginfo-5.5.14-112.1
php5-phar-5.5.14-112.1
php5-wddx-debuginfo-5.5.14-112.1
php5-bz2-debuginfo-5.5.14-112.1
php5-posix-debuginfo-5.5.14-112.1
php5-ldap-5.5.14-112.1
php5-gd-debuginfo-5.5.14-112.1
php5-opcache-debuginfo-5.5.14-112.1
php5-iconv-debuginfo-5.5.14-112.1
php5-xmlwriter-debuginfo-5.5.14-112.1
php5-odbc-debuginfo-5.5.14-112.1
php5-intl-debuginfo-5.5.14-112.1
php5-imap-5.5.14-112.1
php5-odbc-5.5.14-112.1
apache2-mod_php5-5.5.14-112.1
php5-pgsql-debuginfo-5.5.14-112.1
php5-suhosin-debuginfo-5.5.14-112.1
php5-ldap-debuginfo-5.5.14-112.1
php5-gettext-5.5.14-112.1
php5-sysvsem-debuginfo-5.5.14-112.1
php5-gmp-5.5.14-112.1
php5-fileinfo-5.5.14-112.1
php5-readline-debuginfo-5.5.14-112.1
php5-sqlite-5.5.14-112.1
php5-ftp-debuginfo-5.5.14-112.1
php5-dba-debuginfo-5.5.14-112.1
php5-openssl-5.5.14-112.1
php5-dom-debuginfo-5.5.14-112.1
php5-ftp-5.5.14-112.1
php5-sysvmsg-5.5.14-112.1
php5-sysvmsg-debuginfo-5.5.14-112.1
php5-calendar-5.5.14-112.1
php5-mssql-debuginfo-5.5.14-112.1
php5-ctype-5.5.14-112.1
php5-pcntl-debuginfo-5.5.14-112.1

171071 - Amazon Linux AMI ALAS-2019-1165 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6974, CVE-2019-7221, CVE-2019-7222

Description

The scan detected that the host is missing the following update:

ALAS-2019-1165

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://alas.aws.amazon.com/ALAS-2019-1165.html

Amazon Linux AMI
x86_64
perf-debuginfo-4.14.101-75.76.amzn1
kernel-4.14.101-75.76.amzn1
kernel-debuginfo-4.14.101-75.76.amzn1
kernel-tools-devel-4.14.101-75.76.amzn1
kernel-debuginfo-common-x86_64-4.14.101-75.76.amzn1
kernel-devel-4.14.101-75.76.amzn1
kernel-headers-4.14.101-75.76.amzn1
kernel-tools-4.14.101-75.76.amzn1
kernel-tools-debuginfo-4.14.101-75.76.amzn1
perf-4.14.101-75.76.amzn1

i686
perf-debuginfo-4.14.101-75.76.amzn1
kernel-4.14.101-75.76.amzn1
kernel-debuginfo-4.14.101-75.76.amzn1
kernel-tools-devel-4.14.101-75.76.amzn1
kernel-debuginfo-common-i686-4.14.101-75.76.amzn1
kernel-devel-4.14.101-75.76.amzn1
kernel-headers-4.14.101-75.76.amzn1
kernel-tools-4.14.101-75.76.amzn1
kernel-tools-debuginfo-4.14.101-75.76.amzn1
perf-4.14.101-75.76.amzn1

194835 - Fedora Linux 29 FEDORA-2019-15f5147b27 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-8904, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907

Description

The scan detected that the host is missing the following update:
FEDORA-2019-15f5147b27

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 29

file-5.34-12.fc29

194836 - Fedora Linux 28 FEDORA-2019-21b76d179e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-2755, CVE-2018-2758, CVE-2018-2759, CVE-2018-2761, CVE-2018-2762, CVE-2018-2766, CVE-2018-2767, CVE-2018-2769, CVE-2018-2771, CVE-2018-2773, CVE-2018-2775, CVE-2018-2776, CVE-2018-2777, CVE-2018-2778, CVE-2018-2779, CVE-2018-2780, CVE-2018-2781, CVE-2018-2782, CVE-2018-2784, CVE-2018-2786, CVE-2018-2787, CVE-2018-2810, CVE-2018-2812, CVE-2018-2813, CVE-2018-2816, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819, CVE-2018-2839, CVE-2018-2846, CVE-2018-3056, CVE-2018-3058, CVE-2018-3060, CVE-2018-3061, CVE-2018-3062, CVE-2018-3064, CVE-2018-3065, CVE-2018-3066, CVE-2018-3070, CVE-2018-3071, CVE-2018-3077, CVE-2018-3081, CVE-2018-3133, CVE-2018-3143, CVE-2018-3144, CVE-2018-3155, CVE-2018-3156, CVE-2018-3161, CVE-2018-3162, CVE-2018-3171, CVE-2018-3173, CVE-2018-3185, CVE-2018-3187, CVE-2018-3200, CVE-2018-3247, CVE-2018-3251, CVE-2018-3276, CVE-2018-3277, CVE-2018-3278, CVE-2018-3282, CVE-2018-3283, CVE-2018-3284, CVE-2019-2420, CVE-2019-2434, CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2486, CVE-2019-2503, CVE-2019-2507, CVE-2019-2510, CVE-2019-2528, CVE-2019-2529, CVE-2019-2531, CVE-2019-2532, CVE-2019-2534, CVE-2019-2537

Description

The scan detected that the host is missing the following update:
FEDORA-2019-21b76d179e

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 28

community-mysql-5.7.25-1.fc28

194837 - Fedora Linux 29 FEDORA-2019-caab5920f2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3825

Description

The scan detected that the host is missing the following update:
FEDORA-2019-caab5920f2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

gdm-3.30.3-1.fc29

194850 - Fedora Linux 28 FEDORA-2019-6092f8c0dc Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-7572, CVE-2019-7573, CVE-2019-7574, CVE-2019-7575, CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635, CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

Description

The scan detected that the host is missing the following update:

FEDORA-2019-6092f8c0dc

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

SDL-1.2.15-31.fc28

24791 - (JSA10897) Juniper Junos OS J-web Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0062

Description

A denial of service vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in the Juniper device.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in J-Web service. Successful exploitation could allow an attacker to cause a denial of service condition on the targeted system.

24797 - Joomla XSS Issue In Core.js WriteDynaList Vulnerability (20190205)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2019-7740

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw lies in the core.js writeDynaList. Successful exploitation could allow an attacker to affect the integrity of the target system.

89007 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-062-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2018-14647, CVE-2019-5010

Description

The scan detected that the host is missing the following update:
SSA:2019-062-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2019&m=slackware-security.428727

Slackware 14.0
x86_64
python-2.7.16-x86_64-1

Slackware 14.2
x86_64
python-2.7.16-x86_64-1

i586
python-2.7.16-i586-1

Slackware 14.1
x86_64
python-2.7.16-x86_64-1

131306 - Debian Linux 9.0 DSA-4402-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-20743

Description

The scan detected that the host is missing the following update:
DSA-4402-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4402

Debian 9.0
all
mumble_1.2.18-1+deb9u1

147678 - SuSE Linux 42.3 openSUSE-SU-2019:0292-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-14647, CVE-2019-5010

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0292-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00024.html

SuSE Linux 42.3
i586
python-tk-2.7.13-27.12.1
python-gdbm-debuginfo-2.7.13-27.12.1
python-xml-debuginfo-2.7.13-27.12.1
python-2.7.13-27.12.1
python-curses-2.7.13-27.12.1
python-base-debuginfo-2.7.13-27.12.1
libpython2_7-1_0-2.7.13-27.12.1
libpython2_7-1_0-debuginfo-2.7.13-27.12.1
python-demo-2.7.13-27.12.1
python-base-debugsource-2.7.13-27.12.1
python-curses-debuginfo-2.7.13-27.12.1
python-debugsource-2.7.13-27.12.1
python-debuginfo-2.7.13-27.12.1
python-tk-debuginfo-2.7.13-27.12.1
python-devel-2.7.13-27.12.1
python-base-2.7.13-27.12.1
python-idle-2.7.13-27.12.1
python-gdbm-2.7.13-27.12.1
python-xml-2.7.13-27.12.1

noarch
python-doc-2.7.13-27.12.1
python-doc-pdf-2.7.13-27.12.1

x86_64
libpython2_7-1_0-debuginfo-32bit-2.7.13-27.12.1
python-tk-2.7.13-27.12.1
python-gdbm-debuginfo-2.7.13-27.12.1
libpython2_7-1_0-32bit-2.7.13-27.12.1
python-xml-debuginfo-2.7.13-27.12.1
python-2.7.13-27.12.1
python-debuginfo-32bit-2.7.13-27.12.1
python-curses-2.7.13-27.12.1
python-32bit-2.7.13-27.12.1
python-base-debuginfo-2.7.13-27.12.1
libpython2_7-1_0-2.7.13-27.12.1
libpython2_7-1_0-debuginfo-2.7.13-27.12.1
python-demo-2.7.13-27.12.1
python-base-debugsource-2.7.13-27.12.1
python-curses-debuginfo-2.7.13-27.12.1
python-debugsource-2.7.13-27.12.1
python-debuginfo-2.7.13-27.12.1
python-tk-debuginfo-2.7.13-27.12.1
python-devel-2.7.13-27.12.1
python-base-2.7.13-27.12.1
python-idle-2.7.13-27.12.1
python-base-debuginfo-32bit-2.7.13-27.12.1
python-gdbm-2.7.13-27.12.1
python-xml-2.7.13-27.12.1
python-base-32bit-2.7.13-27.12.1

182922 - FreeBSD slixmpp Improper Access Control (526d9642-3ae7-11e9-a669-8c164582fbac)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1000021

Description

The scan detected that the host is missing the following update:
slixmpp -- improper access control (526d9642-3ae7-11e9-a669-8c164582fbac)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/526d9642-3ae7-11e9-a669-8c164582fbac.html

Affected packages:
py35-slixmpp < 1.4.2
py36-slixmpp < 1.4.2
py37-slixmpp < 1.4.2

182925 - FreeBSD py-gunicorn CWE-113 Vulnerability (a3e24de7-3f0c-11e9-87d1-00012e582166)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-1000164

Description

The scan detected that the host is missing the following update:
py-gunicorn -- CWE-113 vulnerability (a3e24de7-3f0c-11e9-87d1-00012e582166)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/a3e24de7-3f0c-11e9-87d1-00012e582166.html

Affected packages:
py27-gunicorn < 19.5.0
py35-gunicorn < 19.5.0
py36-gunicorn < 19.5.0
py37-gunicorn < 19.5.0

186596 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3885-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-6111

Description

The scan detected that the host is missing the following update:
USN-3885-2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004788.html

Ubuntu 16.04

openssh-client_7.2p2-4ubuntu2.8

Ubuntu 18.10

openssh-client_7.7p1-4ubuntu0.3

Ubuntu 14.04

openssh-client_6.6p1-2ubuntu2.13

Ubuntu 18.04

openssh-client_7.6p1-4ubuntu0.3

194830 - Fedora Linux 29 FEDORA-2019-ec55814c1c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3498, CVE-2019-6975

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ec55814c1c

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 29

python-django-2.0.13-1.fc29

194839 - Fedora Linux 28 FEDORA-2019-2f47af13f6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-8955

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2f47af13f6

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=1

Fedora Core 28

tor-0.3.4.11-1.fc28

194844 - Fedora Linux 29 FEDORA-2019-55db688ba9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-8955

Description

The scan detected that the host is missing the following update:
FEDORA-2019-55db688ba9

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

tor-0.3.5.8-1.fc29

194848 - Fedora Linux 28 FEDORA-2019-9760933547 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-3498, CVE-2019-6975

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9760933547

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 28

python-django-2.0.13-1.fc28

194849 - Fedora Linux 29 FEDORA-2019-614f1cd5a8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-3133, CVE-2018-3137, CVE-2018-3143, CVE-2018-3144, CVE-2018-3145, CVE-2018-3155, CVE-2018-3156, CVE-2018-3161, CVE-2018-3162, CVE-2018-3170, CVE-2018-3171, CVE-2018-3173, CVE-2018-3174, CVE-2018-3182, CVE-2018-3185, CVE-2018-3186, CVE-2018-3187, CVE-2018-3195, CVE-2018-3200, CVE-2018-3203, CVE-2018-3212, CVE-2018-3247, CVE-2018-3251, CVE-2018-3276, CVE-2018-3277, CVE-2018-3278, CVE-2018-3279, CVE-2018-3280, CVE-2018-3282, CVE-2018-3283, CVE-2018-3284, CVE-2018-3285, CVE-2018-3286, CVE-2019-2420, CVE-2019-2434, CVE-2019-2436, CVE-2019-2455, CVE-2019-2481, CVE-2019-2482, CVE-2019-2486, CVE-2019-2494, CVE-2019-2495, CVE-2019-2502, CVE-2019-2503, CVE-2019-2507, CVE-2019-2510, CVE-2019-2528, CVE-2019-2529, CVE-2019-2530, CVE-2019-2531, CVE-2019-2532, CVE-2019-2533, CVE-2019-2534, CVE-2019-2535, CVE-2019-2536, CVE-2019-2537, CVE-2019-2539

Description

The scan detected that the host is missing the following update:
FEDORA-2019-614f1cd5a8

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

community-mysql-8.0.15-1.fc29

24800 - IBM AIX Tcpdump Vulnerability (ibm10873086)

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-19519

Description

A vulnerability is present in some versions of IBM AIX.

Observation

AIX is a Unix-like operating system developed by IBM.

A vulnerability is present in some versions of IBM AIX. The flaw lies in tcpdump. Successful exploitation could allow an attacker to overflow a buffer and execute arbitrary code.

24802 - Joomla Lack Of URL Filtering In Various Core Components Vulnerability (20190201)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2019-7744

Description

A cross-site scripting vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A cross-site scripting vulnerability is present in some versions of Joomla! CMS. The flaw lies in various core components. Successful exploitation could allow an attacker to affect the integrity of the target system.

24803 - Joomla Global Configuration helpurl Settings Cross-Site Scripting Vulnerability (20190204)

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2019-7741

Description

A vulnerability is present in some versions of Joomla! CMS.

Observation

Joomla! CMS is an open source content management system.

A vulnerability is present in some versions of Joomla! CMS. The flaw lies in the Global Configuration helpurl settings. Successful

exploitation could allow an attacker to affect the integrity of the target system.

131305 - Debian Linux 9.0 DSA-4400-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1559

Description

The scan detected that the host is missing the following update:
DSA-4400-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4400

Debian 9.0
all
libcrypto1.0.2-udeb_1.0.2r-1~deb9u1
libssl1.0-dev_1.0.2r-1~deb9u1
libssl1.0.2_1.0.2r-1~deb9u1
libssl1.0.2-udeb_1.0.2r-1~deb9u1

147686 - SuSE Linux 42.3 openSUSE-SU-2019:0275-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-5383

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0275-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-03/msg00006.html

SuSE Linux 42.3
noarch
ucode-amd-20170530-26.1
kernel-firmware-20170530-26.1

160526 - CentOS 7 CESA-2019-0464 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:

CESA-2019-0464

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023214.html

CentOS 7
x86_64
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-headless-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.211-2.6.17.1.el7_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el7_6

160527 - CentOS 7 CESA-2019-0436 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
CESA-2019-0436

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.centos.org/pipermail/centos-announce/2019-March/023212.html

CentOS 7
x86_64
java-11-openjdk-devel-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-11.0.2.7-0.el7_6
java-11-openjdk-debug-11.0.2.7-0.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-11.0.2.7-0.el7_6
java-11-openjdk-headless-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.el7_6
java-11-openjdk-devel-11.0.2.7-0.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.el7_6
java-11-openjdk-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.el7_6

i686
java-11-openjdk-devel-debug-11.0.2.7-0.el7_6

java-11-openjdk-jmods-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-11.0.2.7-0.el7_6
java-11-openjdk-debug-11.0.2.7-0.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-11.0.2.7-0.el7_6
java-11-openjdk-headless-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.el7_6
java-11-openjdk-devel-11.0.2.7-0.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.el7_6
java-11-openjdk-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.el7_6

163814 - Oracle Enterprise Linux ELSA-2019-0435 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-3639, CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ELSA-2019-0435

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008507.html
http://oss.oracle.com/pipermail/el-errata/2019-March/008504.html

OEL7
x86_64
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-headless-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-zip-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.201.b09-0.el7_6

163815 - Oracle Enterprise Linux ELSA-2019-0462 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ELSA-2019-0462

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008514.html

OEL6
x86_64
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.0.1.el6_10

i386
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.0.1.el6_10
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.0.1.el6_10

163816 - Oracle Enterprise Linux ELSA-2019-0464 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ELSA-2019-0464

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008513.html

OEL7
x86_64
java-1.7.0-openjdk-headless-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.0.1.el7_6
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.0.1.el7_6

163817 - Oracle Enterprise Linux ELSA-2019-0436 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
ELSA-2019-0436

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2019-March/008505.html

OEL7
x86_64
java-11-openjdk-devel-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.0.1.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-jmods-11.0.2.7-0.0.1.el7_6
java-11-openjdk-11.0.2.7-0.0.1.el7_6
java-11-openjdk-src-11.0.2.7-0.0.1.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.0.1.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-headless-11.0.2.7-0.0.1.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.0.1.el7_6
java-11-openjdk-devel-11.0.2.7-0.0.1.el7_6
java-11-openjdk-demo-11.0.2.7-0.0.1.el7_6

182921 - FreeBSD Node.js Multiple Vulnerabilities (b71d7193-3c54-11e9-a3f9-00155d006b02)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1559, CVE-2019-5737, CVE-2019-5739

Description

The scan detected that the host is missing the following update:
Node.js -- multiple vulnerabilities (b71d7193-3c54-11e9-a3f9-00155d006b02)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/b71d7193-3c54-11e9-a3f9-00155d006b02.html

Affected packages:
node < 11.10.1
node10 < 10.15.2
node8 < 8.15.1
node6 < 6.17.0

186593 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3899-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1559

Description

The scan detected that the host is missing the following update:
USN-3899-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004785.html

Ubuntu 16.04

libssl1.0.0_1.0.2g-1ubuntu4.15

Ubuntu 18.10

libssl1.0.0_1.0.2n-1ubuntu6.2

Ubuntu 18.04

libssl1.0.0_1.0.2n-1ubuntu5.3

186594 - Ubuntu Linux 18.04 USN-3901-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-18397, CVE-2018-19854, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3901-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004789.html

Ubuntu 18.04

linux-image-4.15.0-1030-kvm_4.15.0-1030.30
linux-image-4.15.0-46-generic-lpae_4.15.0-46.49
linux-image-4.15.0-1034-oem_4.15.0-1034.39
linux-image-lowlatency_4.15.0.46.48
linux-image-oracle_4.15.0.1009.12
linux-image-4.15.0-46-generic_4.15.0-46.49
linux-image-generic_4.15.0.46.48
linux-image-4.15.0-46-snapdragon_4.15.0-46.49
linux-image-gke_4.15.0.1028.30
linux-image-4.15.0-46-lowlatency_4.15.0-46.49
linux-image-4.15.0-1009-oracle_4.15.0-1009.11
linux-image-kvm_4.15.0.1030.30
linux-image-generic-lpae_4.15.0.46.48
linux-image-gcp_4.15.0.1028.30

linux-image-4.15.0-1033-aws_4.15.0-1033.35
linux-image-aws_4.15.0.1033.32
linux-image-snapdragon_4.15.0.46.48
linux-image-oem_4.15.0.1034.39
linux-image-raspi2_4.15.0.1032.30
linux-image-4.15.0-1032-raspi2_4.15.0-1032.34
linux-image-4.15.0-1028-gcp_4.15.0-1028.29

186595 - Ubuntu Linux 14.04, 16.04 USN-3901-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-18397, CVE-2018-19854, CVE-2019-6133

Description

The scan detected that the host is missing the following update:
USN-3901-2

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-March/004790.html

Ubuntu 14.04

linux-image-4.15.0-1040-azure_4.15.0-1040.44~14.04.1
linux-image-azure_4.15.0.1040.27

Ubuntu 16.04

linux-image-oem_4.15.0.46.67
linux-image-generic-lpae-hwe-16.04_4.15.0.46.67
linux-image-4.15.0-46-generic_4.15.0-46.49~16.04.1
linux-image-aws-hwe_4.15.0.1033.34
linux-image-4.15.0-1033-aws_4.15.0-1033.35~16.04.1
linux-image-lowlatency-hwe-16.04_4.15.0.46.67
linux-image-gke_4.15.0.1028.42
linux-image-4.15.0-1040-azure_4.15.0-1040.44
linux-image-generic-hwe-16.04_4.15.0.46.67
linux-image-gcp_4.15.0.1028.42
linux-image-4.15.0-1009-oracle_4.15.0-1009.11~16.04.1
linux-image-azure_4.15.0.1040.44
linux-image-4.15.0-1028-gcp_4.15.0-1028.29~16.04.1
linux-image-4.15.0-46-lowlatency_4.15.0-46.49~16.04.1
linux-image-oracle_4.15.0.1009.3
linux-image-4.15.0-46-generic-lpae_4.15.0-46.49~16.04.1

194843 - Fedora Linux 29 FEDORA-2019-b3aec99d2c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-16368, CVE-2018-7173, CVE-2018-7174, CVE-2018-7175, CVE-2018-7452, CVE-2018-7454

Description

The scan detected that the host is missing the following update:

FEDORA-2019-b3aec99d2c

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 29

xpdf-4.01-1.fc29

196260 - Red Hat Enterprise Linux RHSA-2019-0436 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0436

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-February/msg00036.html

RHEL7D
x86_64
java-11-openjdk-devel-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-11.0.2.7-0.el7_6
java-11-openjdk-headless-11.0.2.7-0.el7_6
java-11-openjdk-debug-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.el7_6
java-11-openjdk-debuginfo-11.0.2.7-0.el7_6
java-11-openjdk-devel-11.0.2.7-0.el7_6
java-11-openjdk-src-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.el7_6
java-11-openjdk-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.el7_6

RHEL7S
x86_64
java-11-openjdk-devel-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.el7_6

java-11-openjdk-demo-11.0.2.7-0.el7_6
java-11-openjdk-headless-11.0.2.7-0.el7_6
java-11-openjdk-debug-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.el7_6
java-11-openjdk-debuginfo-11.0.2.7-0.el7_6
java-11-openjdk-devel-11.0.2.7-0.el7_6
java-11-openjdk-src-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.el7_6
java-11-openjdk-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.el7_6

RHEL7WS
x86_64
java-11-openjdk-devel-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-debug-11.0.2.7-0.el7_6
java-11-openjdk-jmods-debug-11.0.2.7-0.el7_6
java-11-openjdk-src-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-debug-11.0.2.7-0.el7_6
java-11-openjdk-headless-debug-11.0.2.7-0.el7_6
java-11-openjdk-demo-11.0.2.7-0.el7_6
java-11-openjdk-headless-11.0.2.7-0.el7_6
java-11-openjdk-debug-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-11.0.2.7-0.el7_6
java-11-openjdk-debuginfo-11.0.2.7-0.el7_6
java-11-openjdk-devel-11.0.2.7-0.el7_6
java-11-openjdk-src-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-zip-11.0.2.7-0.el7_6
java-11-openjdk-11.0.2.7-0.el7_6
java-11-openjdk-javadoc-debug-11.0.2.7-0.el7_6

196261 - Red Hat Enterprise Linux RHSA-2019-0464 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0464

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00008.html

RHEL7D
x86_64
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-headless-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.211-2.6.17.1.el7_6

noarch

java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el7_6

RHEL7S
noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el7_6

x86_64
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-headless-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.211-2.6.17.1.el7_6

RHEL7WS
x86_64
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-headless-1.7.0.211-2.6.17.1.el7_6
java-1.7.0-openjdk-accessibility-1.7.0.211-2.6.17.1.el7_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el7_6

196262 - Red Hat Enterprise Linux RHSA-2019-0435 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0435

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-February/msg00035.html

RHEL7D
x86_64
java-1.8.0-openjdk-headless-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-1.8.0.201.b09-0.el7_6

java-1.8.0-openjdk-debug-1.8.0.201.b09-0.el7_6

noarch
java-1.8.0-openjdk-javadoc-zip-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-0.el7_6

RHEL7S
noarch
java-1.8.0-openjdk-javadoc-zip-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-0.el7_6

x86_64
java-1.8.0-openjdk-headless-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.201.b09-0.el7_6

RHEL7WS
x86_64
java-1.8.0-openjdk-headless-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-headless-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-accessibility-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debuginfo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-devel-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-demo-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-src-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-debug-1.8.0.201.b09-0.el7_6

noarch
java-1.8.0-openjdk-javadoc-zip-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-zip-debug-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-1.8.0.201.b09-0.el7_6
java-1.8.0-openjdk-javadoc-debug-1.8.0.201.b09-0.el7_6

196263 - Red Hat Enterprise Linux RHSA-2019-0462 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-2422

Description

The scan detected that the host is missing the following update:
RHSA-2019-0462

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00007.html

RHEL6D
i386
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el6_10

x86_64
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10

RHEL6S
i386
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10

noarch
java-1.7.0-openjdk-javadoc-1.7.0.211-2.6.17.1.el6_10

x86_64
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-demo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-src-1.7.0.211-2.6.17.1.el6_10

RHEL6WS
x86_64
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10

i386
java-1.7.0-openjdk-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-devel-1.7.0.211-2.6.17.1.el6_10
java-1.7.0-openjdk-debuginfo-1.7.0.211-2.6.17.1.el6_10

131302 - Debian Linux 9.0 DSA-4399-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-9187

Description

The scan detected that the host is missing the following update:
DSA-4399-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4399

Debian 9.0
all
ikiwiki_3.20170111.1

131303 - Debian Linux 9.0 DSA-4397-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3824

Description

The scan detected that the host is missing the following update:
DSA-4397-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2019/dsa-4397

Debian 9.0
all
python-ldb-dev_2:1.1.27-1+deb9u1
ldb-tools_2:1.1.27-1+deb9u1
libldb1_2:1.1.27-1+deb9u1
libldb-dev_2:1.1.27-1+deb9u1
python-ldb_2:1.1.27-1+deb9u1

147681 - SuSE Linux 15.0 openSUSE-SU-2019:0254-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-16872, CVE-2018-18954, CVE-2018-19364, CVE-2018-19489, CVE-2019-6778

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0254-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.opensuse.org/opensuse-updates/2019-02/msg00156.html

SuSE Linux 15.0
x86_64
qemu-arm-debuginfo-2.11.2-lp150.7.18.1
qemu-linux-user-2.11.2-lp150.7.18.1
qemu-ppc-debuginfo-2.11.2-lp150.7.18.1
qemu-block-iscsi-debuginfo-2.11.2-lp150.7.18.1
qemu-linux-user-debuginfo-2.11.2-lp150.7.18.1
qemu-guest-agent-debuginfo-2.11.2-lp150.7.18.1
qemu-block-ssh-2.11.2-lp150.7.18.1
qemu-tools-debuginfo-2.11.2-lp150.7.18.1
qemu-block-rbd-debuginfo-2.11.2-lp150.7.18.1
qemu-lang-2.11.2-lp150.7.18.1
qemu-x86-debuginfo-2.11.2-lp150.7.18.1
qemu-ksm-2.11.2-lp150.7.18.1
qemu-block-iscsi-2.11.2-lp150.7.18.1
qemu-extra-debuginfo-2.11.2-lp150.7.18.1
qemu-2.11.2-lp150.7.18.1
qemu-block-gluster-debuginfo-2.11.2-lp150.7.18.1
qemu-block-dmg-2.11.2-lp150.7.18.1
qemu-debuginfo-2.11.2-lp150.7.18.1
qemu-s390-debuginfo-2.11.2-lp150.7.18.1
qemu-block-rbd-2.11.2-lp150.7.18.1
qemu-extra-2.11.2-lp150.7.18.1
qemu-tools-2.11.2-lp150.7.18.1
qemu-block-dmg-debuginfo-2.11.2-lp150.7.18.1
qemu-ppc-2.11.2-lp150.7.18.1
qemu-s390-2.11.2-lp150.7.18.1
qemu-debugsource-2.11.2-lp150.7.18.1
qemu-arm-2.11.2-lp150.7.18.1
qemu-x86-2.11.2-lp150.7.18.1
qemu-testsuite-2.11.2-lp150.7.18.1
qemu-guest-agent-2.11.2-lp150.7.18.1
qemu-kvm-2.11.2-lp150.7.18.1
qemu-block-ssh-debuginfo-2.11.2-lp150.7.18.1
qemu-block-curl-2.11.2-lp150.7.18.1
qemu-linux-user-debugsource-2.11.2-lp150.7.18.1
qemu-block-gluster-2.11.2-lp150.7.18.1
qemu-block-curl-debuginfo-2.11.2-lp150.7.18.1

noarch
qemu-seabios-1.11.0-lp150.7.18.1
qemu-sgabios-8-lp150.7.18.1
qemu-ipxe-1.0.0+-lp150.7.18.1
qemu-vgabios-1.11.0-lp150.7.18.1

182923 - FreeBSD mybb Vulnerabilities (395ed9d5-3cca-11e9-9ba0-4c72b94353b5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
mybb -- vulnerabilities (395ed9d5-3cca-11e9-9ba0-4c72b94353b5)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/395ed9d5-3cca-11e9-9ba0-4c72b94353b5.html

Affected packages:
mybb < 1.8.20_1

182924 - FreeBSD asterisk Remote Crash Vulnerability With SDP Protocol Violation (be0e3817-3bfe-11e9-9cd6-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-7251

Description

The scan detected that the host is missing the following update:
asterisk -- Remote crash vulnerability with SDP protocol violation (be0e3817-3bfe-11e9-9cd6-001999f8d30b)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/be0e3817-3bfe-11e9-9cd6-001999f8d30b.html

Affected packages:
asterisk15 < 15.7.2
asterisk16 < 16.2.1

182926 - FreeBSD Gitlab Multiple Vulnerabilities (11292460-3f2f-11e9-adcb-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-9170, CVE-2019-9171, CVE-2019-9172, CVE-2019-9174, CVE-2019-9175, CVE-2019-9176, CVE-2019-9178, CVE-2019-9179, CVE-2019-9217, CVE-2019-9219, CVE-2019-9220, CVE-2019-9221, CVE-2019-9222, CVE-2019-9223, CVE-2019-9224, CVE-2019-9225, CVE-2019-9485

Description

The scan detected that the host is missing the following update:
Gitlab -- Multiple vulnerabilities (11292460-3f2f-11e9-adcb-001b217b3468)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/11292460-3f2f-11e9-adcb-001b217b3468.html

Affected packages:
11.8.0 <= gitlab-ce < 11.8.1
11.7.0 <= gitlab-ce < 11.7.6
2.9.0 <= gitlab-ce < 11.6.10

186590 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3898-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-18508

Description

The scan detected that the host is missing the following update:
USN-3898-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004784.html

Ubuntu 16.04

libnss3_3.28.4-0ubuntu0.16.04.5

Ubuntu 18.10

libnss3_3.36.1-1ubuntu1.2

Ubuntu 14.04

libnss3_3.28.4-0ubuntu0.14.04.5

Ubuntu 18.04

libnss3_3.35-2ubuntu2.2

194831 - Fedora Linux 28 FEDORA-2019-c602845b91 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2018-18508

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c602845b91

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 28

nss-3.42.1-1.fc28

194841 - Fedora Linux 28 FEDORA-2019-f0add5eed0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f0add5eed0

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=2

Fedora Core 28

openocd-0.10.0-11.fc28

194842 - Fedora Linux 29 FEDORA-2019-7d1a63acc8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-3828

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7d1a63acc8

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/3/?count=200&page=3

Fedora Core 29

ansible-2.7.8-1.fc29

196259 - Red Hat Enterprise Linux RHSA-2019-0442 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2019-0442

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2019-March/msg00000.html

RHEL6_4S
x86_64
redhat-release-server-6Server-6.4.0.9.el6_4.3

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

24356 - Mozilla Firefox Multiple Vulnerabilities Prior To 63

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2018-12388, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12398, CVE-2018-12399, CVE-2018-12400, CVE-2018-12401, CVE-2018-12402, CVE-2018-12403

Update Details

Risk is updated

24357 - Mozilla Firefox Multiple Vulnerabilities Prior To 63

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-12388, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12398, CVE-2018-12399, CVE-2018-12400, CVE-2018-12401, CVE-2018-12402, CVE-2018-12403

Update Details

Risk is updated

147337 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:3646-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393

Update Details

Risk is updated

147350 - SuSE SLED 15 SUSE-SU-2018:3769-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393

Update Details

Risk is updated

182822 - FreeBSD mozilla Multiple Vulnerabilities (7c3a02b9-3273-4426-a0ba-f90fad2ff72e)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12388, CVE-2018-12390, CVE-2018-12391, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12398, CVE-2018-12399, CVE-2018-12400, CVE-2018-12401, CVE-2018-12402, CVE-2018-12403

Update Details

Risk is updated

131231 - Debian Linux 9.0 DSA-4324-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

131243 - Debian Linux 9.0 DSA-4337-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393

Update Details

Risk is updated

160478 - CentOS 7 CESA-2018-3005 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

160479 - CentOS 6 CESA-2018-3006 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

163724 - Oracle Enterprise Linux ELSA-2018-3005 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

175463 - Scientific Linux Security ERRATA Critical: firefox on SL7.x x86_64 (1810-12458)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

175464 - Scientific Linux Security ERRATA Critical: firefox on SL6.x i386/x86_64 (1810-12900)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

182912 - FreeBSD FreeBSD File Description Reference Count Leak (86c89abf-2d91-11e9-bf3e-a4badb2f4699)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2019-5596

Update Details

Risk is updated

186491 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3801-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12388, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397, CVE-2018-12398, CVE-2018-12399, CVE-2018-12401, CVE-2018-12402, CVE-2018-12403

Update Details

Risk is updated

196129 - Red Hat Enterprise Linux RHSA-2018-3005 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

196170 - Red Hat Enterprise Linux RHSA-2018-3006 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397

Update Details

Risk is updated

131263 - Debian Linux 9.0 DSA-4357-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11759

Update Details

Risk is updated

147433 - SuSE Linux 15.0 openSUSE-SU-2018:4032-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11759

Update Details

Risk is updated

147441 - SuSE SLES 12 SP3 SUSE-SU-2018:3963-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2018-11759

Update Details

Risk is updated

182918 - FreeBSD OpenSSL Undisclosed Vulnerability (7700061f-34f7-11e9-b95c-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-1559

Update Details

Risk is updated CVE is updated

194786 - Fedora Linux 29 FEDORA-2019-af3d726d38 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-7639

Update Details

Risk is updated

194800 - Fedora Linux 28 FEDORA-2019-710afd062a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2019-7639

Update Details

Risk is updated

182914 - FreeBSD FreeBSD System Call Kernel Data Register Leak (683c714d-2d91-11e9-bf3e-a4badb2f4699)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2019-5595

Update Details

Risk is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2019 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates