

MCAFFEE 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

195124 - Fedora Linux 28 FEDORA-2019-a6cd583a8d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16880, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701, CVE-2019-3882, CVE-2019-3900, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9500, CVE-2019-9503, CVE-2019-9857

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a6cd583a8d

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/2019/5/?count=200&page=1>

Fedora Core 28

kernel-5.0.11-100.fc28

195123 - Fedora Linux 29 FEDORA-2019-6174b47003 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6174b47003

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/2019/5/?count=200&page=2>

Fedora Core 29

runc-1.0.0-92.dev.gitc1b8c57.fc29

195125 - Fedora Linux 30 FEDORA-2019-bc70b381ad Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-bc70b381ad

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/2019/5/?count=200&page=3>

Fedora Core 30

runc-1.0.0-92.dev.gitc1b8c57.fc30

25072 - Oracle WebLogic Server Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2018-1258, CVE-2019-2568, CVE-2019-2615, CVE-2019-2618, CVE-2019-2645, CVE-2019-2646, CVE-2019-2647, CVE-2019-2648, CVE-2019-2649, CVE-2019-2650, CVE-2019-2658

Description

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server.

Observation

Oracle WebLogic Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in several components. Successful exploitation could allow an attacker to disclose sensitive information or cause denial of service condition on the target system.

25077 - (APSB19-20) Vulnerabilities In Adobe Shockwave Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-7098, CVE-2019-7099, CVE-2019-7100, CVE-2019-7101, CVE-2019-7102, CVE-2019-7103, CVE-2019-7104

Description

Multiple vulnerabilities are present in some versions of Adobe Shockwave Player.

Observation

Adobe Shockwave Player is a software to view multimedia files created with Adobe Director.

Multiple vulnerabilities are present in some versions of Adobe Shockwave Player. There are multiple memory corruption vulnerabilities

in different components of the affected Shockwave Player. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.

25084 - Oracle Database Server Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2019-2516, CVE-2019-2517, CVE-2019-2518, CVE-2019-2571, CVE-2019-2582, CVE-2019-2619

Description

Multiple vulnerabilities are present in some versions of Oracle Database Server.

Observation

Oracle Database Server is an industrial standard database solution.

Multiple vulnerabilities are present in some versions of Oracle Database Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to compromise Portable Clusterware, Core RDBMS, RDBMS DataPump and Java VM on the target.

25086 - Oracle JDeveloper Critical Patch Update April 2019

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

Risk Level: High

CVE: CVE-2015-9251, CVE-2017-5645, CVE-2018-14718

Description

Multiple vulnerabilities are present in some versions of Oracle JDeveloper.

Observation

Oracle JDeveloper is a popular development framework for Java applications.

Multiple vulnerabilities are present in some versions of Oracle JDeveloper. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

131341 - Debian Linux 9.0 DSA-4438-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11365, CVE-2019-11366

Description

The scan detected that the host is missing the following update:
DSA-4438-1

Observation

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

<http://www.debian.org/security/2019/dsa-4438>

Debian 9.0

all
atftp_0.7.git20120829-3.1~deb9u1

132502 - Oracle VM OVMSA-2019-0014 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1066, CVE-2018-10881, CVE-2018-10882, CVE-2019-3701

Description

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

OVMSA-2019-0014

Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2019-May/000936.html>

OVM3.4

x86_64

kernel-uek-4.1.12-124.26.7.el6uek

kernel-uek-firmware-4.1.12-124.26.7.el6uek

147897 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:1181-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-11234, CVE-2019-11235

Description

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

SUSE-SU-2019:1181-1

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-May/005429.html>

SuSE SLES 12 SP3

x86_64

freeradius-server-python-debuginfo-3.0.15-2.11.2

freeradius-server-ldap-debuginfo-3.0.15-2.11.2

freeradius-server-3.0.15-2.11.2

freeradius-server-sqlite-debuginfo-3.0.15-2.11.2

freeradius-server-mysql-debuginfo-3.0.15-2.11.2

freeradius-server-sqlite-3.0.15-2.11.2

freeradius-server-doc-3.0.15-2.11.2

freeradius-server-mysql-3.0.15-2.11.2

freeradius-server-libs-debuginfo-3.0.15-2.11.2

freeradius-server-postgresql-3.0.15-2.11.2

freeradius-server-debugsource-3.0.15-2.11.2

freeradius-server-perl-3.0.15-2.11.2

freeradius-server-postgresql-debuginfo-3.0.15-2.11.2

freeradius-server-python-3.0.15-2.11.2

freeradius-server-krb5-3.0.15-2.11.2
freeradius-server-libs-3.0.15-2.11.2
freeradius-server-debuginfo-3.0.15-2.11.2
freeradius-server-perl-debuginfo-3.0.15-2.11.2
freeradius-server-utils-3.0.15-2.11.2
freeradius-server-ldap-3.0.15-2.11.2
freeradius-server-krb5-debuginfo-3.0.15-2.11.2
freeradius-server-utils-debuginfo-3.0.15-2.11.2

SuSE SLES 12 SP4

x86_64

freeradius-server-python-debuginfo-3.0.15-2.11.2
freeradius-server-ldap-debuginfo-3.0.15-2.11.2
freeradius-server-3.0.15-2.11.2
freeradius-server-sqlite-debuginfo-3.0.15-2.11.2
freeradius-server-mysql-debuginfo-3.0.15-2.11.2
freeradius-server-sqlite-3.0.15-2.11.2
freeradius-server-doc-3.0.15-2.11.2
freeradius-server-mysql-3.0.15-2.11.2
freeradius-server-libs-debuginfo-3.0.15-2.11.2
freeradius-server-postgresql-3.0.15-2.11.2
freeradius-server-debugsource-3.0.15-2.11.2
freeradius-server-perl-3.0.15-2.11.2
freeradius-server-postgresql-debuginfo-3.0.15-2.11.2
freeradius-server-python-3.0.15-2.11.2
freeradius-server-krb5-3.0.15-2.11.2
freeradius-server-libs-3.0.15-2.11.2
freeradius-server-debuginfo-3.0.15-2.11.2
freeradius-server-perl-debuginfo-3.0.15-2.11.2
freeradius-server-utils-3.0.15-2.11.2
freeradius-server-ldap-3.0.15-2.11.2
freeradius-server-krb5-debuginfo-3.0.15-2.11.2
freeradius-server-utils-debuginfo-3.0.15-2.11.2

147898 - SuSE Linux 15.0 openSUSE-SU-2019:1325-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5805, CVE-2019-5806, CVE-2019-5807, CVE-2019-5808, CVE-2019-5809, CVE-2019-5810, CVE-2019-5811, CVE-2019-5812, CVE-2019-5813, CVE-2019-5814, CVE-2019-5815, CVE-2019-5816, CVE-2019-5817, CVE-2019-5818, CVE-2019-5819, CVE-2019-5820, CVE-2019-5821, CVE-2019-5822, CVE-2019-5823

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1325-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00028.html>

SuSE Linux 15.0

x86_64

chromedriver-74.0.3729.108-lp150.209.2
chromium-debugsource-74.0.3729.108-lp150.209.2
chromedriver-debuginfo-74.0.3729.108-lp150.209.2
chromium-74.0.3729.108-lp150.209.2

chromium-debuginfo-74.0.3729.108-lp150.209.2

147899 - SuSE Linux 15.0 openSUSE-SU-2019:1314-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1314-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00013.html>

SuSE Linux 15.0

x86_64

ntfsprogs-debuginfo-2016.2.22-lp150.2.3.1
libntfs-3g-devel-2016.2.22-lp150.2.3.1
ntfsprogs-extra-debuginfo-2016.2.22-lp150.2.3.1
libntfs-3g87-2016.2.22-lp150.2.3.1
ntfsprogs-2016.2.22-lp150.2.3.1
ntfs-3g-debuginfo-2016.2.22-lp150.2.3.1
ntfs-3g_ntfsprogs-debugsource-2016.2.22-lp150.2.3.1
ntfsprogs-extra-2016.2.22-lp150.2.3.1
ntfs-3g_ntfsprogs-debuginfo-2016.2.22-lp150.2.3.1
ntfs-3g-2016.2.22-lp150.2.3.1
libntfs-3g87-debuginfo-2016.2.22-lp150.2.3.1

i586

ntfsprogs-debuginfo-2016.2.22-lp150.2.3.1
libntfs-3g-devel-2016.2.22-lp150.2.3.1
ntfsprogs-extra-debuginfo-2016.2.22-lp150.2.3.1
libntfs-3g87-2016.2.22-lp150.2.3.1
ntfsprogs-2016.2.22-lp150.2.3.1
ntfs-3g-debuginfo-2016.2.22-lp150.2.3.1
ntfs-3g_ntfsprogs-debugsource-2016.2.22-lp150.2.3.1
ntfsprogs-extra-2016.2.22-lp150.2.3.1
ntfs-3g_ntfsprogs-debuginfo-2016.2.22-lp150.2.3.1
ntfs-3g-2016.2.22-lp150.2.3.1
libntfs-3g87-debuginfo-2016.2.22-lp150.2.3.1

147900 - SuSE Linux 42.3 openSUSE-SU-2019:1324-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5805, CVE-2019-5806, CVE-2019-5807, CVE-2019-5808, CVE-2019-5809, CVE-2019-5810, CVE-2019-5811, CVE-2019-5813, CVE-2019-5814, CVE-2019-5815, CVE-2019-5818, CVE-2019-5819, CVE-2019-5820, CVE-2019-5821, CVE-2019-5822, CVE-2019-5823

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1324-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00027.html>

SuSE Linux 42.3

x86_64

chromium-debugsource-74.0.3729.108-208.1

chromedriver-74.0.3729.108-208.1

chromium-debuginfo-74.0.3729.108-208.1

chromedriver-debuginfo-74.0.3729.108-208.1

chromium-74.0.3729.108-208.1

147901 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1136-1 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-2019:1136-1

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-May/005421.html>

SuSE SLED 12 SP3

x86_64

openssl-debuginfo-1.0.2j-60.52.1

libopenssl1_0_0-1.0.2j-60.52.1

openssl-debugsource-1.0.2j-60.52.1

libopenssl-devel-1.0.2j-60.52.1

libopenssl1_0_0-32bit-1.0.2j-60.52.1

openssl-1.0.2j-60.52.1

libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.52.1

libopenssl1_0_0-debuginfo-1.0.2j-60.52.1

SuSE SLES 12 SP3

noarch

openssl-doc-1.0.2j-60.52.1

x86_64

libopenssl1_0_0-hmac-1.0.2j-60.52.1

libopenssl1_0_0-hmac-32bit-1.0.2j-60.52.1

openssl-debuginfo-1.0.2j-60.52.1

libopenssl1_0_0-1.0.2j-60.52.1

openssl-debugsource-1.0.2j-60.52.1

libopenssl-devel-1.0.2j-60.52.1

libopenssl1_0_0-32bit-1.0.2j-60.52.1

openssl-1.0.2j-60.52.1

libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.52.1

libopenssl1_0_0-debuginfo-1.0.2j-60.52.1

147902 - SuSE Linux 42.3 openSUSE-SU-2019:1313-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-9755

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1313-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00014.html>

SuSE Linux 42.3

x86_64

ntfs-3g-2013.1.13-7.6.1

ntfsprogs-debuginfo-2013.1.13-7.6.1

libntfs-3g84-debuginfo-2013.1.13-7.6.1

ntfs-3g-debuginfo-2013.1.13-7.6.1

libntfs-3g-devel-2013.1.13-7.6.1

ntfsprogs-2013.1.13-7.6.1

ntfs-3g_ntfsprogs-debugsource-2013.1.13-7.6.1

libntfs-3g84-2013.1.13-7.6.1

i586

ntfs-3g-2013.1.13-7.6.1

ntfsprogs-debuginfo-2013.1.13-7.6.1

libntfs-3g84-debuginfo-2013.1.13-7.6.1

ntfs-3g-debuginfo-2013.1.13-7.6.1

libntfs-3g-devel-2013.1.13-7.6.1

ntfsprogs-2013.1.13-7.6.1

ntfs-3g_ntfsprogs-debugsource-2013.1.13-7.6.1

libntfs-3g84-2013.1.13-7.6.1

147903 - SuSE Linux 15.0 openSUSE-SU-2019:1310-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12910

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1310-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00016.html>

SuSE Linux 15.0

i586

libsoup-2_4-1-2.62.2-lp150.2.3.1

typelib-1_0-Soup-2_4-2.62.2-lp150.2.3.1
libsoup-devel-2.62.2-lp150.2.3.1
libsoup-2_4-1-debuginfo-2.62.2-lp150.2.3.1
libsoup-debugsource-2.62.2-lp150.2.3.1

noarch
libsoup-lang-2.62.2-lp150.2.3.1

x86_64
libsoup-2_4-1-32bit-debuginfo-2.62.2-lp150.2.3.1
libsoup-2_4-1-2.62.2-lp150.2.3.1
libsoup-devel-2.62.2-lp150.2.3.1
libsoup-2_4-1-32bit-2.62.2-lp150.2.3.1
typelib-1_0-Soup-2_4-2.62.2-lp150.2.3.1
libsoup-debugsource-2.62.2-lp150.2.3.1
libsoup-2_4-1-debuginfo-2.62.2-lp150.2.3.1
libsoup-devel-32bit-2.62.2-lp150.2.3.1

147905 - SuSE Linux 42.3 openSUSE-SU-2019:1316-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-8375

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1316-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00018.html>

SuSE Linux 42.3

i586
webkit2gtk-4_0-injected-bundles-2.24.0-24.1
typelib-1_0-JavaScriptCore-4_0-2.24.0-24.1
libwebkit2gtk-4_0-37-debuginfo-2.24.0-24.1
webkit2gtk3-minibrowser-2.24.0-24.1
webkit2gtk3-devel-2.24.0-24.1
webkit2gtk3-debugsource-2.24.0-24.1
webkit2gtk3-plugin-process-gtk2-2.24.0-24.1
webkit2gtk3-minibrowser-debuginfo-2.24.0-24.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-24.1
webkit-jsc-4-debuginfo-2.24.0-24.1
libwebkit2gtk-4_0-37-2.24.0-24.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.0-24.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-24.1
typelib-1_0-WebKit2-4_0-2.24.0-24.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.0-24.1
libjavascriptcoregtk-4_0-18-2.24.0-24.1
webkit-jsc-4-2.24.0-24.1

noarch
libwebkit2gtk3-lang-2.24.0-24.1

x86_64

webkit2gtk-4_0-injected-bundles-2.24.0-24.1
typelib-1_0-JavaScriptCore-4_0-2.24.0-24.1
libwebkit2gtk-4_0-37-debuginfo-2.24.0-24.1
webkit2gtk3-minibrowser-2.24.0-24.1
webkit2gtk3-devel-2.24.0-24.1
webkit2gtk3-debugsource-2.24.0-24.1
webkit2gtk3-plugin-process-gtk2-2.24.0-24.1
webkit2gtk3-minibrowser-debuginfo-2.24.0-24.1
libjavascriptcoregtk-4_0-18-debuginfo-2.24.0-24.1
webkit-jsc-4-debuginfo-2.24.0-24.1
libwebkit2gtk-4_0-37-2.24.0-24.1
libwebkit2gtk-4_0-37-32bit-2.24.0-24.1
typelib-1_0-WebKit2WebExtension-4_0-2.24.0-24.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.0-24.1
libjavascriptcoregtk-4_0-18-debuginfo-32bit-2.24.0-24.1
libjavascriptcoregtk-4_0-18-32bit-2.24.0-24.1
typelib-1_0-WebKit2-4_0-2.24.0-24.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.24.0-24.1
libwebkit2gtk-4_0-37-debuginfo-32bit-2.24.0-24.1
libjavascriptcoregtk-4_0-18-2.24.0-24.1
webkit-jsc-4-2.24.0-24.1

147912 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:1141-1 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-2019:1141-1

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-May/005422.html>

SuSE SLED 12 SP4

x86_64

libopenssl1_1-32bit-1.1.1b-2.12.2
libopenssl1_1-debuginfo-32bit-1.1.1b-2.12.2
libopenssl1_1-debuginfo-1.1.1b-2.12.2
openssl-1_1-debugsource-1.1.1b-2.12.2
openssl-1_1-debuginfo-1.1.1b-2.12.2
libopenssl1_1-1.1.1b-2.12.2

SuSE SLES 12 SP4

x86_64

libopenssl1_1-32bit-1.1.1b-2.12.2
libopenssl1_1-debuginfo-32bit-1.1.1b-2.12.2
libopenssl1_1-debuginfo-1.1.1b-2.12.2
openssl-1_1-debugsource-1.1.1b-2.12.2
openssl-1_1-debuginfo-1.1.1b-2.12.2
libopenssl1_1-1.1.1b-2.12.2

182973 - FreeBSD comms/hylafax Malformed Fax Sender Remote Code Execution In JPEG Support (3df5a920-6edc-11e9-

a44b-0050562a4d7b)

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

Risk Level: High

CVE: CVE-2018-17141

Description

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

comms/hylafax -- Malformed fax sender remote code execution in JPEG support (3df5a920-6edc-11e9-a44b-0050562a4d7b)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/3df5a920-6edc-11e9-a44b-0050562a4d7b.html>

Affected packages:

hylafax < 6.0.7

186684 - Ubuntu Linux 16.04 USN-3968-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7076, CVE-2017-1000368

Description

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

USN-3968-1

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-May/004880.html>

Ubuntu 16.04

sudo-ldap_1.8.16-0ubuntu1.6

sudo_1.8.16-0ubuntu1.6

195120 - Fedora Linux 30 FEDORA-2019-d29e04fa11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-10877, CVE-2019-10878, CVE-2019-10879

Description

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

FEDORA-2019-d29e04fa11

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/2019/5/?count=200&page=1>

Fedora Core 30

teeworlds-0.7.3.1-2.fc30

195140 - Fedora Linux 28 FEDORA-2019-1a3edd7e8a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6930, CVE-2017-6931, CVE-2018-7600, CVE-2018-7602, CVE-2018-9861, CVE-2019-10909, CVE-2019-10910, CVE-2019-10911, CVE-2019-11358

Description

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

FEDORA-2019-1a3edd7e8a

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/2019/5/?count=200&page=1>

Fedora Core 28

drupal8-8.6.15-1.fc28

195145 - Fedora Linux 29 FEDORA-2019-8219efa9f6 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-2019-3882, CVE-2019-3900, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-8912, CVE-2019-8980, CVE-2019-9500, CVE-2019-9503, CVE-2019-9857

Description

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

FEDORA-2019-8219efa9f6

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/2019/5/?count=200&page=2>

Fedora Core 29

kernel-5.0.10-200.fc29

196305 - Red Hat Enterprise Linux RHSA-2019-1024 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5226, CVE-2019-10063

Description

The scan detected that the host is missing the following update:
RHSA-2019-1024

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-May/msg00015.html>

RHEL7D

x86_64
flatpak-1.0.2-5.el7_6
flatpak-debuginfo-1.0.2-5.el7_6
flatpak-libs-1.0.2-5.el7_6
flatpak-builder-1.0.0-5.el7_6
flatpak-devel-1.0.2-5.el7_6

RHEL7S

x86_64
flatpak-1.0.2-5.el7_6
flatpak-debuginfo-1.0.2-5.el7_6
flatpak-libs-1.0.2-5.el7_6
flatpak-builder-1.0.0-5.el7_6
flatpak-devel-1.0.2-5.el7_6

RHEL7WS

x86_64
flatpak-1.0.2-5.el7_6
flatpak-debuginfo-1.0.2-5.el7_6
flatpak-libs-1.0.2-5.el7_6
flatpak-builder-1.0.0-5.el7_6
flatpak-devel-1.0.2-5.el7_6

196306 - Red Hat Enterprise Linux RHSA-2019-1021 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5805, CVE-2019-5806, CVE-2019-5807, CVE-2019-5808, CVE-2019-5809, CVE-2019-5810, CVE-2019-5811, CVE-2019-5813, CVE-2019-5814, CVE-2019-5815, CVE-2019-5818, CVE-2019-5819, CVE-2019-5820, CVE-2019-5821, CVE-2019-5822, CVE-2019-5823

Description

The scan detected that the host is missing the following update:
RHSA-2019-1021

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-May/msg00014.html>

RHEL6D

i386
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

i686
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

x86_64
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

RHEL6S
i386
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

i686
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

x86_64
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

RHEL6WS
i386
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

i686
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

x86_64
chromium-browser-74.0.3729.108-1.el6_10
chromium-browser-debuginfo-74.0.3729.108-1.el6_10

25085 - (JSA10925) Juniper Junos OS Firewall Filter Terms Named "internal-1" and "internal-2" Being Ignored Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0036

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in firewall filter terms named using the format "internal-n". Successful exploitation could allow an attacker to bypass certain security restrictions.

147896 - SuSE Linux 42.3 openSUSE-SU-2019:1320-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16412, CVE-2018-16413, CVE-2018-16644, CVE-2018-20467, CVE-2019-10650, CVE-2019-11007, CVE-2019-11008, CVE-2019-11009, CVE-2019-7175, CVE-2019-7395, CVE-2019-7397, CVE-2019-7398, CVE-2019-9956

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1320-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00023.html>

SuSE Linux 42.3

i586

ImageMagick-debugsource-6.8.8.1-82.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-82.1
ImageMagick-devel-6.8.8.1-82.1
libMagickCore-6_Q16-1-6.8.8.1-82.1
ImageMagick-debuginfo-6.8.8.1-82.1
libMagick+-6_Q16-3-6.8.8.1-82.1
ImageMagick-extra-6.8.8.1-82.1
libMagick+-devel-6.8.8.1-82.1
libMagick+-6_Q16-3-debuginfo-6.8.8.1-82.1
ImageMagick-config-6-upstream-6.8.8.1-82.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-82.1
perl-PerlMagick-debuginfo-6.8.8.1-82.1
libMagickWand-6_Q16-1-6.8.8.1-82.1
ImageMagick-6.8.8.1-82.1
ImageMagick-config-6-SUSE-6.8.8.1-82.1
perl-PerlMagick-6.8.8.1-82.1
ImageMagick-extra-debuginfo-6.8.8.1-82.1

noarch

ImageMagick-doc-6.8.8.1-82.1

x86_64

ImageMagick-debugsource-6.8.8.1-82.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-82.1
libMagick+-6_Q16-3-32bit-6.8.8.1-82.1
ImageMagick-devel-6.8.8.1-82.1
libMagickCore-6_Q16-1-6.8.8.1-82.1
ImageMagick-debuginfo-6.8.8.1-82.1
libMagick+-6_Q16-3-6.8.8.1-82.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-82.1
libMagickWand-6_Q16-1-32bit-6.8.8.1-82.1
ImageMagick-extra-6.8.8.1-82.1
libMagick+-devel-6.8.8.1-82.1
ImageMagick-devel-32bit-6.8.8.1-82.1
libMagick+-6_Q16-3-debuginfo-6.8.8.1-82.1
libMagickWand-6_Q16-1-debuginfo-32bit-6.8.8.1-82.1
libMagick+-6_Q16-3-debuginfo-32bit-6.8.8.1-82.1
ImageMagick-config-6-upstream-6.8.8.1-82.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-82.1
perl-PerlMagick-debuginfo-6.8.8.1-82.1
libMagickWand-6_Q16-1-6.8.8.1-82.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-82.1
ImageMagick-6.8.8.1-82.1
ImageMagick-config-6-SUSE-6.8.8.1-82.1
perl-PerlMagick-6.8.8.1-82.1
ImageMagick-extra-debuginfo-6.8.8.1-82.1
libMagick+-devel-32bit-6.8.8.1-82.1

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

Risk Level: Medium

CVE: CVE-2019-10650, CVE-2019-11007, CVE-2019-11008, CVE-2019-9956

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1331-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00029.html>

SuSE Linux 15.0

i586

ImageMagick-config-7-SUSE-7.0.7.34-lp150.2.29.1
ImageMagick-debuginfo-7.0.7.34-lp150.2.29.1
ImageMagick-config-7-upstream-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-7_Q16HDR14-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-devel-7.0.7.34-lp150.2.29.1
ImageMagick-extra-debuginfo-7.0.7.34-lp150.2.29.1
ImageMagick-extra-7.0.7.34-lp150.2.29.1
perl-PerlMagick-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-7_Q16HDR14-7.0.7.34-lp150.2.29.1
ImageMagick-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.29.1
ImageMagick-devel-7.0.7.34-lp150.2.29.1
ImageMagick-debugsource-7.0.7.34-lp150.2.29.1
perl-PerlMagick-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDR16-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDR16-7.0.7.34-lp150.2.29.1

noarch

ImageMagick-doc-7.0.7.34-lp150.2.29.1

x86_64

libMagick++-7_Q16HDR14-32bit-7.0.7.34-lp150.2.29.1
ImageMagick-config-7-SUSE-7.0.7.34-lp150.2.29.1
ImageMagick-debuginfo-7.0.7.34-lp150.2.29.1
ImageMagick-config-7-upstream-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-7_Q16HDR14-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-devel-7.0.7.34-lp150.2.29.1
ImageMagick-extra-debuginfo-7.0.7.34-lp150.2.29.1
ImageMagick-extra-7.0.7.34-lp150.2.29.1
ImageMagick-devel-32bit-7.0.7.34-lp150.2.29.1
perl-PerlMagick-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-7_Q16HDR14-7.0.7.34-lp150.2.29.1
ImageMagick-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDR16-debuginfo-7.0.7.34-lp150.2.29.1
libMagick++-7_Q16HDR14-32bit-debuginfo-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDR16-32bit-7.0.7.34-lp150.2.29.1
libMagick++-devel-32bit-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDR16-32bit-7.0.7.34-lp150.2.29.1
ImageMagick-devel-7.0.7.34-lp150.2.29.1

ImageMagick-debugsource-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDRI6-32bit-debuginfo-7.0.7.34-lp150.2.29.1
perl-PerlMagick-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDRI6-32bit-debuginfo-7.0.7.34-lp150.2.29.1
libMagickWand-7_Q16HDRI6-7.0.7.34-lp150.2.29.1
libMagickCore-7_Q16HDRI6-7.0.7.34-lp150.2.29.1

171092 - Amazon Linux AMI ALAS-2019-1200 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3877, CVE-2019-3878

Description

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

ALAS-2019-1200

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2019-1200.html>

Amazon Linux AMI

x86_64

mod24_auth_mellon-0.14.0-2.8.amzn1

mod24_auth_mellon-debuginfo-0.14.0-2.8.amzn1

mod24_auth_mellon-diagnostics-0.14.0-2.8.amzn1

i686

mod24_auth_mellon-0.14.0-2.8.amzn1

mod24_auth_mellon-debuginfo-0.14.0-2.8.amzn1

mod24_auth_mellon-diagnostics-0.14.0-2.8.amzn1

186682 - Ubuntu Linux 18.04, 18.10, 19.04 USN-3967-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-15822, CVE-2019-11338, CVE-2019-11339, CVE-2019-9718, CVE-2019-9721

Description

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

USN-3967-1

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-May/004879.html>

Ubuntu 18.10

libavformat58_4.0.4-0ubuntu1

libavresample4_4.0.4-0ubuntu1

libpostproc55_4.0.4-0ubuntu1

libswscale5_4.0.4-0ubuntu1

libavcodec58_4.0.4-0ubuntu1
libswresample3_4.0.4-0ubuntu1
libavdevice58_4.0.4-0ubuntu1
ffmpeg_4.0.4-0ubuntu1
libavutil56_4.0.4-0ubuntu1
libavfilter-extra7_4.0.4-0ubuntu1
libavfilter7_4.0.4-0ubuntu1
libavcodec-extra58_4.0.4-0ubuntu1

Ubuntu 19.04

libavutil56_4.1.3-0ubuntu1
libswscale5_4.1.3-0ubuntu1
ffmpeg_4.1.3-0ubuntu1
libavdevice58_4.1.3-0ubuntu1
libavfilter-extra7_4.1.3-0ubuntu1
libavformat58_4.1.3-0ubuntu1
libavfilter7_4.1.3-0ubuntu1
libswresample3_4.1.3-0ubuntu1
libavcodec58_4.1.3-0ubuntu1
libavresample4_4.1.3-0ubuntu1
libavcodec-extra58_4.1.3-0ubuntu1
libpostproc55_4.1.3-0ubuntu1

Ubuntu 18.04

libswscale4_3.4.6-0ubuntu0.18.04.1
libavfilter6_3.4.6-0ubuntu0.18.04.1
libavcodec-extra57_3.4.6-0ubuntu0.18.04.1
libavfilter-extra6_3.4.6-0ubuntu0.18.04.1
ffmpeg_3.4.6-0ubuntu0.18.04.1
libavresample3_3.4.6-0ubuntu0.18.04.1
libswresample2_3.4.6-0ubuntu0.18.04.1
libavutil55_3.4.6-0ubuntu0.18.04.1
libavcodec57_3.4.6-0ubuntu0.18.04.1
libavformat57_3.4.6-0ubuntu0.18.04.1
libpostproc54_3.4.6-0ubuntu0.18.04.1
libavdevice57_3.4.6-0ubuntu0.18.04.1

195121 - Fedora Linux 29 FEDORA-2019-219b0b0b6a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1098, CVE-2018-1099, CVE-2018-16886

Description

The scan detected that the host is missing the following update:
FEDORA-2019-219b0b0b6a

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/2019/5/?count=200&page=2>

Fedora Core 29

etcd-3.3.12-4.20190413gitf29b1ad.fc29

195138 - Fedora Linux 30 FEDORA-2019-87d807d7cb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3900

Description

The scan detected that the host is missing the following update:
FEDORA-2019-87d807d7cb

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/2019/5/?count=200&page=3>

Fedora Core 30

kernel-5.0.10-300.fc30

195148 - Fedora Linux 30 FEDORA-2019-521e6c567c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11023

Description

The scan detected that the host is missing the following update:
FEDORA-2019-521e6c567c

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/2019/5/?count=200&page=2>

Fedora Core 30

graphviz-2.40.1-46.fc30

196307 - Red Hat Enterprise Linux RHSA-2019-1017 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3839, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
RHSA-2019-1017

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-May/msg00013.html>

RHEL7D

x86_64
ghostscript-gtk-9.07-31.el7_6.11
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11
ghostscript-cups-9.07-31.el7_6.11
ghostscript-debuginfo-9.07-31.el7_6.11

noarch
ghostscript-doc-9.07-31.el7_6.11

RHEL7S

noarch
ghostscript-doc-9.07-31.el7_6.11

x86_64
ghostscript-gtk-9.07-31.el7_6.11
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11
ghostscript-cups-9.07-31.el7_6.11
ghostscript-debuginfo-9.07-31.el7_6.11

RHEL7WS

x86_64
ghostscript-gtk-9.07-31.el7_6.11
ghostscript-devel-9.07-31.el7_6.11
ghostscript-9.07-31.el7_6.11
ghostscript-cups-9.07-31.el7_6.11
ghostscript-debuginfo-9.07-31.el7_6.11

noarch
ghostscript-doc-9.07-31.el7_6.11

25075 - (JSA10926) Juniper Junos OS Jdhcpd Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0037

Description

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

Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in the dhcpv6 environment. Successful exploitation could allow a remote attacker to cause a denial of service condition in the target system.

25083 - IBM HTTP Server Multiple Vulnerabilities (ibm10880413)

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

Risk Level: Medium

CVE: CVE-2019-0220

Description

A vulnerability is present in some versions of IBM HTTP Server.

Observation

IBM HTTP Server is an Apache-based web server.

A vulnerability is present in some versions of IBM HTTP Server. The flaw is due to URL normalization inconsistencies. Successful exploitation could allow an attacker to bypass security restrictions and perform unauthorized actions on the target.

25090 - (JSA10933) Juniper Junos OS EX4300-MP Series Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2019-0041

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw is triggered when network traffic reaches the control panel through loopback interface. Successful exploitation could allow an attacker to bypass security restrictions on the target system.

147906 - SuSE Linux 15.0 openSUSE-SU-2019:1315-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9396, CVE-2018-19539, CVE-2018-19542

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1315-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00017.html>

SuSE Linux 15.0

x86_64

jasper-2.0.14-lp150.2.3.1

jasper-debuginfo-2.0.14-lp150.2.3.1

libjasper4-debuginfo-2.0.14-lp150.2.3.1

libjasper4-32bit-2.0.14-lp150.2.3.1

libjasper4-32bit-debuginfo-2.0.14-lp150.2.3.1

libjasper4-2.0.14-lp150.2.3.1

libjasper-devel-2.0.14-lp150.2.3.1

jasper-debugsource-2.0.14-lp150.2.3.1

i586

jasper-2.0.14-lp150.2.3.1

jasper-debuginfo-2.0.14-lp150.2.3.1

libjasper4-debuginfo-2.0.14-lp150.2.3.1
libjasper4-2.0.14-lp150.2.3.1
libjasper-devel-2.0.14-lp150.2.3.1
jasper-debugsource-2.0.14-lp150.2.3.1

147907 - SuSE Linux 15.0 openSUSE-SU-2019:1327-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-2602, CVE-2019-2684

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:1327-1

Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00025.html>

SuSE Linux 15.0

x86_64

java-11-openjdk-accessibility-11.0.3.0-lp150.2.16.1
java-11-openjdk-headless-11.0.3.0-lp150.2.16.1
java-11-openjdk-accessibility-debuginfo-11.0.3.0-lp150.2.16.1
java-11-openjdk-debugsource-11.0.3.0-lp150.2.16.1
java-11-openjdk-src-11.0.3.0-lp150.2.16.1
java-11-openjdk-demo-11.0.3.0-lp150.2.16.1
java-11-openjdk-debuginfo-11.0.3.0-lp150.2.16.1
java-11-openjdk-devel-11.0.3.0-lp150.2.16.1
java-11-openjdk-11.0.3.0-lp150.2.16.1
java-11-openjdk-jmods-11.0.3.0-lp150.2.16.1

noarch

java-11-openjdk-javadoc-11.0.3.0-lp150.2.16.1

147908 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:1166-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5186

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1166-1

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-May/005428.html>

SuSE SLED 12 SP3

x86_64

libaudit1-2.8.1-8.3.1

libauparse0-debuginfo-2.8.1-8.3.1
audit-debugsource-2.8.1-8.3.1
libauparse0-2.8.1-8.3.1
libaudit1-debuginfo-2.8.1-8.3.1
audit-2.8.1-8.3.3
libaudit1-debuginfo-32bit-2.8.1-8.3.1
libaudit1-32bit-2.8.1-8.3.1

SuSE SLES 12 SP3

x86_64
libaudit1-2.8.1-8.3.1
libauparse0-debuginfo-2.8.1-8.3.1
audit-debugsource-2.8.1-8.3.1
libauparse0-2.8.1-8.3.1
libaudit1-debuginfo-2.8.1-8.3.1
audit-2.8.1-8.3.3
libaudit1-debuginfo-32bit-2.8.1-8.3.1
audit-audispd-plugins-2.8.1-8.3.3
libaudit1-32bit-2.8.1-8.3.1

147910 - SuSE Linux 15.0 openSUSE-SU-2019:1312-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10691

Description

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

openSUSE-SU-2019:1312-1

Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-05/msg00012.html>

SuSE Linux 15.0

x86_64
dovecot23-fts-2.3.3-lp150.11.1
dovecot23-2.3.3-lp150.11.1
dovecot23-fts-solr-debuginfo-2.3.3-lp150.11.1
dovecot23-backend-mysql-debuginfo-2.3.3-lp150.11.1
dovecot23-fts-lucene-2.3.3-lp150.11.1
dovecot23-fts-squat-debuginfo-2.3.3-lp150.11.1
dovecot23-fts-solr-2.3.3-lp150.11.1
dovecot23-backend-mysql-2.3.3-lp150.11.1
dovecot23-backend-pgsql-2.3.3-lp150.11.1
dovecot23-fts-lucene-debuginfo-2.3.3-lp150.11.1
dovecot23-backend-sqlite-debuginfo-2.3.3-lp150.11.1
dovecot23-devel-2.3.3-lp150.11.1
dovecot23-backend-pgsql-debuginfo-2.3.3-lp150.11.1
dovecot23-fts-debuginfo-2.3.3-lp150.11.1
dovecot23-debugsource-2.3.3-lp150.11.1
dovecot23-debuginfo-2.3.3-lp150.11.1
dovecot23-fts-squat-2.3.3-lp150.11.1
dovecot23-backend-sqlite-2.3.3-lp150.11.1

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

Risk Level: Medium

CVE: CVE-2019-11070, CVE-2019-6201, CVE-2019-6251, CVE-2019-7285, CVE-2019-7292, CVE-2019-8503, CVE-2019-8506, CVE-2019-8515, CVE-2019-8524, CVE-2019-8535, CVE-2019-8536, CVE-2019-8544, CVE-2019-8551, CVE-2019-8558, CVE-2019-8559, CVE-2019-8563

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1155-1

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-May/005426.html>

SuSE SLES 12 SP3

x86_64
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-2.41.5
webkit2gtk3-debugsource-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-2.24.1-2.41.5
libwebkit2gtk-4_0-37-debuginfo-2.24.1-2.41.5
libwebkit2gtk-4_0-37-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-2.41.5
typelib-1_0-JavaScriptCore-4_0-2.24.1-2.41.5
typelib-1_0-WebKit2-4_0-2.24.1-2.41.5
webkit2gtk-4_0-injected-bundles-2.24.1-2.41.5

SuSE SLES 12 SP4

x86_64
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-2.41.5
webkit2gtk3-debugsource-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-2.24.1-2.41.5
libwebkit2gtk-4_0-37-debuginfo-2.24.1-2.41.5
libwebkit2gtk-4_0-37-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-2.41.5
typelib-1_0-JavaScriptCore-4_0-2.24.1-2.41.5
typelib-1_0-WebKit2-4_0-2.24.1-2.41.5
webkit2gtk-4_0-injected-bundles-2.24.1-2.41.5

SuSE SLED 12 SP4

x86_64
webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-2.41.5
webkit2gtk3-debugsource-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-2.24.1-2.41.5
libwebkit2gtk-4_0-37-debuginfo-2.24.1-2.41.5
libwebkit2gtk-4_0-37-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-2.41.5
typelib-1_0-JavaScriptCore-4_0-2.24.1-2.41.5
typelib-1_0-WebKit2-4_0-2.24.1-2.41.5
webkit2gtk-4_0-injected-bundles-2.24.1-2.41.5

noarch
libwebkit2gtk3-lang-2.24.1-2.41.5

SuSE SLED 12 SP3

x86_64

webkit2gtk-4_0-injected-bundles-debuginfo-2.24.1-2.41.5
webkit2gtk3-debugsource-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-2.24.1-2.41.5
libwebkit2gtk-4_0-37-debuginfo-2.24.1-2.41.5
libwebkit2gtk-4_0-37-2.24.1-2.41.5
libjavascriptcoregtk-4_0-18-debuginfo-2.24.1-2.41.5
typelib-1_0-JavaScriptCore-4_0-2.24.1-2.41.5
typelib-1_0-WebKit2-4_0-2.24.1-2.41.5
webkit2gtk-4_0-injected-bundles-2.24.1-2.41.5

noarch
libwebkit2gtk3-lang-2.24.1-2.41.5

171093 - Amazon Linux AMI ALAS-2019-1202 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20406, CVE-2019-9636

Description

The scan detected that the host is missing the following update:
ALAS-2019-1202

Observation

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

<https://alas.aws.amazon.com/ALAS-2019-1202.html>

Amazon Linux AMI

x86_64
python34-debuginfo-3.4.10-1.43.amzn1
python34-libs-3.4.10-1.43.amzn1
python34-devel-3.4.10-1.43.amzn1
python34-tools-3.4.10-1.43.amzn1
python34-test-3.4.10-1.43.amzn1
python34-3.4.10-1.43.amzn1

i686
python34-debuginfo-3.4.10-1.43.amzn1
python34-libs-3.4.10-1.43.amzn1
python34-test-3.4.10-1.43.amzn1
python34-tools-3.4.10-1.43.amzn1
python34-3.4.10-1.43.amzn1
python34-devel-3.4.10-1.43.amzn1

186678 - Ubuntu Linux 18.04, 18.10, 19.04 USN-3963-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11596

Description

The scan detected that the host is missing the following update:
USN-3963-1

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-May/004873.html>

Ubuntu 18.10

memcached_1.5.10-0ubuntu1.18.10.1

Ubuntu 19.04

memcached_1.5.10-0ubuntu1.19.04.1

Ubuntu 18.04

memcached_1.5.6-0ubuntu1.1

186681 - Ubuntu Linux 18.04, 18.10, 19.04 USN-3964-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12020, CVE-2019-6690

Description

The scan detected that the host is missing the following update:
USN-3964-1

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-May/004876.html>

Ubuntu 18.10

python3-gnupg_0.4.1-1ubuntu1.18.10.1

python-gnupg_0.4.1-1ubuntu1.18.10.1

Ubuntu 19.04

python3-gnupg_0.4.3-1ubuntu1.19.04.1

python-gnupg_0.4.3-1ubuntu1.19.04.1

Ubuntu 18.04

python3-gnupg_0.4.1-1ubuntu1.18.04.1

python-gnupg_0.4.1-1ubuntu1.18.04.1

195141 - Fedora Linux 28 FEDORA-2019-e71f6f36ac Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16877, CVE-2018-16878, CVE-2019-3885

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e71f6f36ac

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/2019/5/?count=200&page=2>

Fedora Core 28

pacemaker-1.1.18-3.fc28

195142 - Fedora Linux 29 FEDORA-2019-b502250ba4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16877, CVE-2018-16878, CVE-2019-3885

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b502250ba4

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/2019/5/?count=200&page=2>

Fedora Core 29

pacemaker-2.0.0-5.fc29

195143 - Fedora Linux 30 FEDORA-2019-0f4190cdb0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-6109, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0f4190cdb0

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/2019/5/?count=200&page=2>

Fedora Core 30

openssh-8.0p1-1.fc30

195147 - Fedora Linux 28 FEDORA-2019-d9f867cb65 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12545

Description

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

FEDORA-2019-d9f867cb65

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/2019/5/?count=200&page=3>

Fedora Core 28

jetty-9.4.11-3.v20180605.fc28

196304 - Red Hat Enterprise Linux RHSA-2019-1022 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10745

Description

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

RHSA-2019-1022

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2019-May/msg00012.html>

RHEL7D

noarch

python-jinja2-2.7.2-3.el7_6

RHEL7S

noarch

python-jinja2-2.7.2-3.el7_6

RHEL7WS

noarch

python-jinja2-2.7.2-3.el7_6

171091 - Amazon Linux AMI ALAS-2019-1201 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3459, CVE-2019-3460, CVE-2019-7308

Description

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

ALAS-2019-1201

Observation

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

<https://alas.aws.amazon.com/ALAS-2019-1201.html>

Amazon Linux AMI

x86_64

kernel-headers-4.14.114-82.97.amzn1
kernel-tools-devel-4.14.114-82.97.amzn1
kernel-debuginfo-4.14.114-82.97.amzn1
kernel-tools-debuginfo-4.14.114-82.97.amzn1
kernel-tools-4.14.114-82.97.amzn1
kernel-4.14.114-82.97.amzn1
kernel-devel-4.14.114-82.97.amzn1
perf-4.14.114-82.97.amzn1
kernel-debuginfo-common-x86_64-4.14.114-82.97.amzn1
perf-debuginfo-4.14.114-82.97.amzn1

i686

perf-4.14.114-82.97.amzn1
kernel-debuginfo-4.14.114-82.97.amzn1
kernel-headers-4.14.114-82.97.amzn1
kernel-tools-debuginfo-4.14.114-82.97.amzn1
kernel-debuginfo-common-i686-4.14.114-82.97.amzn1
kernel-4.14.114-82.97.amzn1
kernel-devel-4.14.114-82.97.amzn1
kernel-tools-4.14.114-82.97.amzn1
kernel-tools-devel-4.14.114-82.97.amzn1
perf-debuginfo-4.14.114-82.97.amzn1

186679 - Ubuntu Linux 16.04, 18.04, 18.10, 19.04 USN-3969-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11555

Description

The scan detected that the host is missing the following update:
USN-3969-1

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-May/004881.html>

Ubuntu 16.04

hostapd_2.4-0ubuntu6.5
wpasupplicant_2.4-0ubuntu6.5

Ubuntu 18.10

hostapd_2.6-18ubuntu1.2
wpasupplicant_2.6-18ubuntu1.2

Ubuntu 19.04

wpasupplicant_2.6-21ubuntu3.1
hostapd_2.6-21ubuntu3.1

Ubuntu 18.04

hostapd_2.6-15ubuntu2.3
wpasupplicant_2.6-15ubuntu2.3

195117 - Fedora Linux 30 FEDORA-2019-eba8e44ee6 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-10909, CVE-2019-10910, CVE-2019-10911, CVE-2019-11358

Description

The scan detected that the host is missing the following update:
FEDORA-2019-eba8e44ee6

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/2019/5/?count=200&page=1>

Fedora Core 30

drupal8-8.6.15-1.fc30

195126 - Fedora Linux 28 FEDORA-2019-902786bc1e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11065

Description

The scan detected that the host is missing the following update:
FEDORA-2019-902786bc1e

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/2019/5/?count=200&page=3>

Fedora Core 28

gradle-4.3.1-9.fc28

195127 - Fedora Linux 28 FEDORA-2019-3193a75b06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18267, CVE-2018-13988, CVE-2019-11026, CVE-2019-9903

Description

The scan detected that the host is missing the following update:
FEDORA-2019-3193a75b06

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/2019/5/?count=200&page=2>

Fedora Core 28

poppler-0.62.0-22.fc28

195129 - Fedora Linux 28 FEDORA-2019-c701e6605a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c701e6605a

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/2019/5/?count=200&page=3>

Fedora Core 28

java-1.8.0-openjdk-1.8.0.212.b04-0.fc28

195132 - Fedora Linux 28 FEDORA-2019-79cb2bb18e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11372, CVE-2019-11373

Description

The scan detected that the host is missing the following update:
FEDORA-2019-79cb2bb18e

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/2019/5/?count=200&page=3>

Fedora Core 28

libmediainfo-18.12-3.fc28

195135 - Fedora Linux 29 FEDORA-2019-9d1e542c57 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-11372, CVE-2019-11373

Description

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

FEDORA-2019-9d1e542c57

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/2019/5/?count=200&page=3>

Fedora Core 29

libmediainfo-18.12-3.fc29

195139 - Fedora Linux 29 FEDORA-2019-ec644ec323 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3639

Description

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

FEDORA-2019-ec644ec323

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/2019/5/?count=200&page=2>

Fedora Core 29

java-1.8.0-openjdk-1.8.0.212.b04-0.fc29

25071 - (K32840424) F5 BIG-IP APM XSS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2019-6591

Description

A vulnerability is present in some versions of F5 BIG-IP systems.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in BIG-IP APM product configured with full webtop.

Successful exploitation could allow an attacker to remotely inject arbitrary code on the target system.

132501 - Oracle VM OVMSA-2019-0015 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13305

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0015

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2019-May/000937.html>

OVM3.4
x86_64
kernel-uek-4.1.12-124.26.10.el6uek
kernel-uek-firmware-4.1.12-124.26.10.el6uek

182972 - FreeBSD gitea Multiple Vulnerabilities (a1de4ae9-6fda-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:
gitea -- multiple vulnerabilities (a1de4ae9-6fda-11e9-9ba0-4c72b94353b5)

Observation

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

<http://www.vuxml.org/freebsd/a1de4ae9-6fda-11e9-9ba0-4c72b94353b5.html>

Affected packages:
gitea < 1.8.0

182974 - FreeBSD Gitlab Information Disclosure (4faac805-6be0-11e9-a685-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-11605

Description

The scan detected that the host is missing the following update:
Gitlab -- Information Disclosure (4faac805-6be0-11e9-a685-001b217b3468)

Observation

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

<http://www.vuxml.org/freebsd/4faac805-6be0-11e9-a685-001b217b3468.html>

Affected packages:

11.10.0 <= gitlab-ce < 11.10.3

11.9.0 <= gitlab-ce < 11.9.11

11.8.0 <= gitlab-ce < 11.8.10

195118 - Fedora Linux 29 FEDORA-2019-6119518602 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-2019-6119518602

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/2019/5/?count=200&page=3>

Fedora Core 29

php-horde-turba-4.2.24-1.fc29

195119 - Fedora Linux 30 FEDORA-2019-f791948895 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5743

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f791948895

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/2019/5/?count=200&page=2>

Fedora Core 30

bind-dyndb-ldap-11.1-15.fc30

bind-9.11.6-3.P1.fc30

dnisperf-2.2.1-4.fc30

dhcp-4.3.6-34.fc30

195122 - Fedora Linux 28 FEDORA-2019-a975e52e95 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-a975e52e95

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/2019/5/?count=200&page=3>

Fedora Core 28

php-horde-horde-5.2.21-1.fc28

195128 - Fedora Linux 29 FEDORA-2019-b3bfc61567 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3840

Description

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

FEDORA-2019-b3bfc61567

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/2019/5/?count=200&page=2>

Fedora Core 29

libvirt-4.7.0-2.fc29

195130 - Fedora Linux 29 FEDORA-2019-a155364f3c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-8320, CVE-2019-8321, CVE-2019-8322, CVE-2019-8323, CVE-2019-8324, CVE-2019-8325

Description

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

FEDORA-2019-a155364f3c

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/2019/5/?count=200&page=3>

Fedora Core 29

ruby-2.5.5-101.fc29

195131 - Fedora Linux 30 FEDORA-2019-e29ba2d34a 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-e29ba2d34a

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/2019/5/?count=200&page=4>

Fedora Core 30

php-horde-turba-4.2.24-1.fc30

195133 - Fedora Linux 29 FEDORA-2019-d5b80d05b9 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-d5b80d05b9

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/2019/5/?count=200&page=2>

Fedora Core 29

libqb-1.0.5-1.fc29

195134 - Fedora Linux 29 FEDORA-2019-4226584eef 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-2019-4226584eef

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/2019/5/?count=200&page=3>

Fedora Core 29

php-horde-horde-5.2.21-1.fc29

195136 - Fedora Linux 30 FEDORA-2019-d348f5a9e7 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-d348f5a9e7

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/2019/5/?count=200&page=4>

Fedora Core 30

php-horde-horde-5.2.21-1.fc30

195137 - Fedora Linux 30 FEDORA-2019-1911b73cee 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-2019-1911b73cee

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/2019/5/?count=200&page=1>

Fedora Core 30

perl-YAML-1.28-1.fc30

195144 - Fedora Linux 30 FEDORA-2019-5557661da8 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-2019-5557661da8

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/2019/5/?count=200&page=3>

Fedora Core 30

java-1.8.0-openjdk-1.8.0.212.b04-0.fc30

195146 - Fedora Linux 28 FEDORA-2019-146df522df 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-2019-146df522df

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/2019/5/?count=200&page=3>

Fedora Core 28

php-horde-turba-4.2.24-1.fc28

195149 - Fedora Linux 30 FEDORA-2019-a8996fb898 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-a8996fb898

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/2019/5/?count=200&page=2>

Fedora Core 30

java-11-openjdk-11.0.3.7-1.fc30

195150 - Fedora Linux 30 FEDORA-2019-a658c47a7a 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-a658c47a7a

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/2019/5/?count=200&page=2>

Fedora Core 30

bubblewrap-0.3.3-2.fc30

147909 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:1157-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-0161

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:1157-1

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-May/005425.html>

SuSE SLED 12 SP4

noarch
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.16.1

SuSE SLES 12 SP4

noarch
qemu-uefi-aarch64-2017+git1510945757.b2662641d5-3.16.1
qemu-ovmf-x86_64-2017+git1510945757.b2662641d5-3.16.1

x86_64

ovmf-tools-2017+git1510945757.b2662641d5-3.16.1
ovmf-2017+git1510945757.b2662641d5-3.16.1

186683 - Ubuntu Linux 18.10, 19.04 USN-3965-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3500

Description

The scan detected that the host is missing the following update:
USN-3965-1

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-May/004878.html>

Ubuntu 19.04

libaria2-0_1.34.0-3ubuntu0.1
aria2_1.34.0-3ubuntu0.1

Ubuntu 18.10

aria2_1.34.0-2ubuntu0.1
libaria2-0_1.34.0-2ubuntu0.1

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.

147543 - SuSE Linux 42.3 openSUSE-SU-2019:0021-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19456

Update Details

Risk is updated

88988 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-337-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12404

Update Details

Risk is updated

132485 - Oracle VM OVMSA-2018-0264 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

Update Details

Risk is updated

147445 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:4117-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384, CVE-2018-12404

[Update Details](#)

Risk is updated

147655 - SuSE Linux 15.0 openSUSE-SU-2019:0183-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12404

[Update Details](#)

Risk is updated

160462 - CentOS 7 CESA-2018-2768 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

160469 - CentOS 6 CESA-2018-2898 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

163700 - Oracle Enterprise Linux ELSA-2018-2768 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

163709 - Oracle Enterprise Linux ELSA-2018-2898 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

171028 - Amazon Linux AMI ALAS-2018-1095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

175452 - Scientific Linux Security ERRATA Moderate: nss on SL7.x x86_64 (1809-3288)

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

175456 - Scientific Linux Security ERRATA Moderate: nss on SL6.x i386/x86_64 (1810-6985)

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

194164 - Fedora Linux 28 FEDORA-2018-1a7a5c54c2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

194168 - Fedora Linux 27 FEDORA-2018-4a21a8ca59 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

194192 - Fedora Linux 29 FEDORA-2018-c72d2d89ec Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

194562 - Fedora Linux 28 FEDORA-2018-2575edf8d3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12404

[Update Details](#)

Risk is updated

194563 - Fedora Linux 29 FEDORA-2018-a78b2ef820 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12404

[Update Details](#)

Risk is updated

195097 - Fedora Linux 30 FEDORA-2019-7322053e74 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3843

[Update Details](#)

Risk is updated

196097 - Red Hat Enterprise Linux RHSA-2018-2768 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[Update Details](#)

Risk is updated

196114 - Red Hat Enterprise Linux RHSA-2018-2898 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12384

[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.

MCAFFEE 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