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

144948 - SuSE Linux 11.4 openSUSE-SU-2016:2649-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7446, CVE-2015-0272, CVE-2015-1339, CVE-2015-3339, CVE-2015-5307, CVE-2015-6252, CVE-2015-6937, CVE-2015-7509, CVE-2015-7515, CVE-2015-7550, CVE-2015-7566, CVE-2015-7799, CVE-2015-7872, CVE-2015-7990, CVE-2015-8104, CVE-2015-8215, CVE-2015-8539, CVE-2015-8543, CVE-2015-8569, CVE-2015-8575, CVE-2015-8767, CVE-2015-8785, CVE-2015-8812, CVE-2015-8816, CVE-2016-0723, CVE-2016-2069, CVE-2016-2143, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-2384, CVE-2016-2543, CVE-2016-2544, CVE-2016-2545, CVE-2016-2546, CVE-2016-2547, CVE-2016-2548, CVE-2016-2549, CVE-2016-2782, CVE-2016-2847, CVE-2016-3134, CVE-2016-3137, CVE-2016-3138, CVE-2016-3139, CVE-2016-3140, CVE-2016-3156, CVE-2016-4486, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2649-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00102.html

SuSE Linux 11.4
i586
kernel-default-base-debuginfo-3.0.101-105.1
kernel-ec2-devel-debuginfo-3.0.101-105.1
kernel-desktop-hmac-3.0.101-105.1
kernel-xen-debugsource-3.0.101-105.1
kernel-ec2-extra-3.0.101-105.1
kernel-desktop-debugsource-3.0.101-105.1
kernel-default-devel-3.0.101-105.1
kernel-vanilla-devel-debuginfo-3.0.101-105.1
kernel-ec2-debugsource-3.0.101-105.1
kernel-trace-hmac-3.0.101-105.1
kernel-desktop-debuginfo-3.0.101-105.1
kernel-xen-hmac-3.0.101-105.1
kernel-default-hmac-3.0.101-105.1
kernel-default-debuginfo-3.0.101-105.1
kernel-vanilla-debuginfo-3.0.101-105.1
kernel-debug-devel-debuginfo-3.0.101-105.1
kernel-vanilla-debugsource-3.0.101-105.1
kernel-ec2-base-debuginfo-3.0.101-105.1
kernel-trace-devel-debuginfo-3.0.101-105.1
kernel-ec2-devel-3.0.101-105.1
kernel-pae-devel-debuginfo-3.0.101-105.1
kernel-ec2-hmac-3.0.101-105.1

kernel-vmi-debuginfo-3.0.101-105.1
kernel-desktop-devel-debuginfo-3.0.101-105.1
preload-1.2-6.83.1
kernel-desktop-devel-3.0.101-105.1
kernel-trace-base-3.0.101-105.1
kernel-vmi-3.0.101-105.1
kernel-pae-base-3.0.101-105.1
kernel-vanilla-base-debuginfo-3.0.101-105.1
kernel-vmi-hmac-3.0.101-105.1
kernel-xen-3.0.101-105.1
kernel-default-debugsource-3.0.101-105.1
kernel-debug-debuginfo-3.0.101-105.1
kernel-desktop-3.0.101-105.1
kernel-ec2-3.0.101-105.1
kernel-debug-base-3.0.101-105.1
kernel-trace-base-debuginfo-3.0.101-105.1
kernel-vmi-debugsource-3.0.101-105.1
kernel-syms-3.0.101-105.1
preload-kmp-desktop-debuginfo-1.2_3.0.101_105-6.83.1
preload-kmp-default-1.2_3.0.101_105-6.83.1
kernel-ec2-base-3.0.101-105.1
kernel-debug-base-debuginfo-3.0.101-105.1
preload-kmp-default-debuginfo-1.2_3.0.101_105-6.83.1
kernel-vanilla-3.0.101-105.1
kernel-trace-devel-3.0.101-105.1
kernel-debug-debugsource-3.0.101-105.1
kernel-desktop-base-3.0.101-105.1
kernel-xen-devel-3.0.101-105.1
kernel-default-3.0.101-105.1
kernel-vmi-base-debuginfo-3.0.101-105.1
kernel-vanilla-base-3.0.101-105.1
kernel-default-devel-debuginfo-3.0.101-105.1
kernel-desktop-base-debuginfo-3.0.101-105.1
kernel-pae-debuginfo-3.0.101-105.1
kernel-source-vanilla-3.0.101-105.1
kernel-pae-3.0.101-105.1
kernel-xen-debuginfo-3.0.101-105.1
kernel-debug-hmac-3.0.101-105.1
kernel-pae-devel-3.0.101-105.1
kernel-ec2-debuginfo-3.0.101-105.1
kernel-xen-base-3.0.101-105.1
preload-kmp-desktop-1.2_3.0.101_105-6.83.1
preload-debuginfo-1.2-6.83.1
kernel-source-3.0.101-105.1
kernel-vanilla-hmac-3.0.101-105.1
kernel-ec2-extra-debuginfo-3.0.101-105.1
kernel-vmi-devel-3.0.101-105.1
kernel-debug-devel-3.0.101-105.1
kernel-pae-base-debuginfo-3.0.101-105.1
kernel-vmi-base-3.0.101-105.1
preload-debugsource-1.2-6.83.1
kernel-pae-hmac-3.0.101-105.1
kernel-trace-debugsource-3.0.101-105.1
kernel-vmi-devel-debuginfo-3.0.101-105.1
kernel-trace-debuginfo-3.0.101-105.1
kernel-xen-base-debuginfo-3.0.101-105.1
kernel-trace-3.0.101-105.1
kernel-xen-devel-debuginfo-3.0.101-105.1
kernel-pae-debugsource-3.0.101-105.1
kernel-vanilla-devel-3.0.101-105.1

kernel-default-base-3.0.101-105.1
kernel-debug-3.0.101-105.1

noarch
kernel-docs-3.0.101-105.2

x86_64
kernel-default-base-debuginfo-3.0.101-105.1
kernel-ec2-devel-debuginfo-3.0.101-105.1
kernel-desktop-hmac-3.0.101-105.1
kernel-xen-debugsource-3.0.101-105.1
kernel-ec2-extra-3.0.101-105.1
kernel-desktop-debugsource-3.0.101-105.1
kernel-default-devel-3.0.101-105.1
kernel-vanilla-devel-debuginfo-3.0.101-105.1
kernel-ec2-debugsource-3.0.101-105.1
kernel-trace-hmac-3.0.101-105.1
kernel-desktop-debuginfo-3.0.101-105.1
kernel-xen-hmac-3.0.101-105.1
kernel-default-hmac-3.0.101-105.1
kernel-default-debuginfo-3.0.101-105.1
kernel-vanilla-debuginfo-3.0.101-105.1
kernel-debug-devel-debuginfo-3.0.101-105.1
kernel-vanilla-debugsource-3.0.101-105.1
kernel-ec2-base-debuginfo-3.0.101-105.1
kernel-trace-devel-debuginfo-3.0.101-105.1
kernel-ec2-devel-3.0.101-105.1
kernel-ec2-hmac-3.0.101-105.1
kernel-desktop-devel-debuginfo-3.0.101-105.1
preload-1.2-6.83.1
kernel-desktop-devel-3.0.101-105.1
kernel-trace-base-3.0.101-105.1
kernel-vanilla-base-debuginfo-3.0.101-105.1
kernel-xen-3.0.101-105.1
kernel-default-debugsource-3.0.101-105.1
kernel-debug-debuginfo-3.0.101-105.1
kernel-desktop-3.0.101-105.1
kernel-ec2-3.0.101-105.1
kernel-debug-base-3.0.101-105.1
kernel-trace-base-debuginfo-3.0.101-105.1
kernel-syms-3.0.101-105.1
preload-kmp-desktop-debuginfo-1.2_3.0.101_105-6.83.1
preload-kmp-default-1.2_3.0.101_105-6.83.1
kernel-ec2-base-3.0.101-105.1
kernel-debug-base-debuginfo-3.0.101-105.1
preload-kmp-default-debuginfo-1.2_3.0.101_105-6.83.1
kernel-vanilla-3.0.101-105.1
kernel-trace-devel-3.0.101-105.1
kernel-debug-debugsource-3.0.101-105.1
kernel-desktop-base-3.0.101-105.1
kernel-xen-devel-3.0.101-105.1
kernel-default-3.0.101-105.1
kernel-vanilla-base-3.0.101-105.1
kernel-default-devel-debuginfo-3.0.101-105.1
kernel-desktop-base-debuginfo-3.0.101-105.1
kernel-source-vanilla-3.0.101-105.1
kernel-xen-debuginfo-3.0.101-105.1
kernel-debug-hmac-3.0.101-105.1
kernel-ec2-debuginfo-3.0.101-105.1
kernel-xen-base-3.0.101-105.1

preload-kmp-desktop-1.2_3.0.101_105-6.83.1
preload-debuginfo-1.2-6.83.1
kernel-source-3.0.101-105.1
kernel-vanilla-hmac-3.0.101-105.1
kernel-ec2-extra-debuginfo-3.0.101-105.1
kernel-debug-devel-3.0.101-105.1
preload-debugsource-1.2-6.83.1
kernel-trace-debugsource-3.0.101-105.1
kernel-trace-debuginfo-3.0.101-105.1
kernel-xen-base-debuginfo-3.0.101-105.1
kernel-trace-3.0.101-105.1
kernel-xen-devel-debuginfo-3.0.101-105.1
kernel-vanilla-devel-3.0.101-105.1
kernel-default-base-3.0.101-105.1
kernel-debug-3.0.101-105.1

144954 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2650-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2650-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002363.html

SuSE SLES 12 SP1
noarch
libxml2-doc-2.9.1-26.3.1

x86_64
python-libxml2-2.9.1-26.3.1
libxml2-debugsource-2.9.1-26.3.1
libxml2-2-debuginfo-2.9.1-26.3.1
python-libxml2-debuginfo-2.9.1-26.3.1
libxml2-tools-debuginfo-2.9.1-26.3.1
libxml2-2-debuginfo-32bit-2.9.1-26.3.1
python-libxml2-debugsource-2.9.1-26.3.1
libxml2-tools-2.9.1-26.3.1
libxml2-2-2.9.1-26.3.1
libxml2-2-32bit-2.9.1-26.3.1

SuSE SLED 12 SP1
x86_64
python-libxml2-2.9.1-26.3.1
libxml2-debugsource-2.9.1-26.3.1
libxml2-2-debuginfo-2.9.1-26.3.1
python-libxml2-debuginfo-2.9.1-26.3.1
libxml2-tools-debuginfo-2.9.1-26.3.1
libxml2-2-debuginfo-32bit-2.9.1-26.3.1
python-libxml2-debugsource-2.9.1-26.3.1
libxml2-tools-2.9.1-26.3.1

libxml2-2-2.9.1-26.3.1
libxml2-2-32bit-2.9.1-26.3.1

144955 - SuSE SLES 11 SP4 SUSE-SU-2016:2652-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4658

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2652-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002364.html

SuSE SLES 11 SP4
i586
libxml2-2.7.6-0.50.1
libxml2-python-2.7.6-0.50.4
libxml2-doc-2.7.6-0.50.1

x86_64
libxml2-32bit-2.7.6-0.50.1
libxml2-2.7.6-0.50.1
libxml2-python-2.7.6-0.50.4
libxml2-doc-2.7.6-0.50.1

144956 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2653-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2653-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002365.html

SuSE SLES 12 SP1
x86_64
libpython3_4m1_0-3.4.5-17.1
python3-base-3.4.5-17.1
libpython3_4m1_0-debuginfo-3.4.5-17.1
python3-base-debuginfo-3.4.5-17.1
python3-debuginfo-3.4.5-17.1
python3-debugsource-3.4.5-17.1
python3-3.4.5-17.1

python3-base-debugsource-3.4.5-17.1

SuSE SLED 12 SP1
x86_64
libpython3_4m1_0-3.4.5-17.1
python3-base-3.4.5-17.1
libpython3_4m1_0-debuginfo-3.4.5-17.1
python3-base-debuginfo-3.4.5-17.1
python3-debuginfo-3.4.5-17.1
python3-debugsource-3.4.5-17.1
python3-3.4.5-17.1
python3-base-debugsource-3.4.5-17.1

144963 - SuSE Linux 13.2 openSUSE-SU-2016:2625-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7513, CVE-2015-8956, CVE-2016-0823, CVE-2016-1237, CVE-2016-5195, CVE-2016-5696, CVE-2016-6327, CVE-2016-6480, CVE-2016-6828, CVE-2016-7117, CVE-2016-7425, CVE-2016-8658

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2625-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00091.html

SuSE Linux 13.2
i586
ipset-kmp-pae-debuginfo-6.23_k3.16.7_45-22.1
kernel-ec2-3.16.7-45.1
cloop-kmp-desktop-2.639_k3.16.7_45-14.22.1
xen-tools-domU-4.4.4_05-51.2
kernel-default-3.16.7-45.1
kernel-default-devel-3.16.7-45.1
virtualbox-guest-kmp-pae-debuginfo-5.0.28_k3.16.7_45-54.2
crash-debuginfo-7.0.8-22.1
crash-eppic-debuginfo-7.0.8-22.1
python-virtualbox-debuginfo-5.0.28-54.2
pcfclock-kmp-desktop-debuginfo-0.44_k3.16.7_45-260.22.1
bbswitch-kmp-default-0.8_k3.16.7_45-3.22.1
ipset-kmp-pae-6.23_k3.16.7_45-22.1
vhba-kmp-default-debuginfo-20140629_k3.16.7_45-2.22.1
ipset-kmp-default-debuginfo-6.23_k3.16.7_45-22.1
kernel-obs-build-debugsource-3.16.7-45.1
cloop-kmp-default-2.639_k3.16.7_45-14.22.1
cloop-kmp-pae-2.639_k3.16.7_45-14.22.1
vhba-kmp-desktop-debuginfo-20140629_k3.16.7_45-2.22.1
kernel-obs-build-3.16.7-45.1
virtualbox-host-kmp-pae-5.0.28_k3.16.7_45-54.2
virtualbox-websrv-debuginfo-5.0.28-54.2
xtables-addons-kmp-desktop-debuginfo-2.6_k3.16.7_45-24.1
virtualbox-host-kmp-default-5.0.28_k3.16.7_45-54.2
hdjmod-kmp-pae-debuginfo-1.28_k3.16.7_45-18.23.1
ipset-kmp-desktop-6.23_k3.16.7_45-22.1

pcfclock-debuginfo-0.44-260.22.1
xtables-addons-debugsource-2.6-24.1
kernel-ec2-base-3.16.7-45.1
virtualbox-host-kmp-pae-debuginfo-5.0.28_k3.16.7_45-54.2
crash-kmp-pae-debuginfo-7.0.8_k3.16.7_45-22.1
crash-gcore-debuginfo-7.0.8-22.1
python-virtualbox-5.0.28-54.2
virtualbox-devel-5.0.28-54.2
ipset-kmp-xen-6.23_k3.16.7_45-22.1
pcfclock-kmp-desktop-0.44_k3.16.7_45-260.22.1
ipset-debuginfo-6.23-22.1
bbswitch-kmp-pae-debuginfo-0.8_k3.16.7_45-3.22.1
cloop-kmp-pae-debuginfo-2.639_k3.16.7_45-14.22.1
hdjmod-kmp-desktop-1.28_k3.16.7_45-18.23.1
libipset3-6.23-22.1
virtualbox-guest-tools-5.0.28-54.2
kernel-default-debugsource-3.16.7-45.1
cloop-kmp-xen-2.639_k3.16.7_45-14.22.1
ipset-6.23-22.1
xtables-addons-kmp-default-debuginfo-2.6_k3.16.7_45-24.1
kernel-ec2-devel-3.16.7-45.1
virtualbox-host-kmp-desktop-debuginfo-5.0.28_k3.16.7_45-54.2
hdjmod-kmp-xen-1.28_k3.16.7_45-18.23.1
bbswitch-0.8-3.22.1
xen-libs-debuginfo-4.4.4_05-51.2
kernel-default-base-3.16.7-45.1
crash-devel-7.0.8-22.1
vhba-kmp-default-20140629_k3.16.7_45-2.22.1
virtualbox-qt-debuginfo-5.0.28-54.2
virtualbox-websrv-5.0.28-54.2
virtualbox-guest-tools-debuginfo-5.0.28-54.2
xen-libs-4.4.4_05-51.2
pcfclock-kmp-pae-debuginfo-0.44_k3.16.7_45-260.22.1
kernel-syms-3.16.7-45.1
hdjmod-kmp-desktop-debuginfo-1.28_k3.16.7_45-18.23.1
vhba-kmp-pae-20140629_k3.16.7_45-2.22.1
virtualbox-guest-kmp-desktop-5.0.28_k3.16.7_45-54.2
libipset3-debuginfo-6.23-22.1
virtualbox-guest-x11-5.0.28-54.2
xtables-addons-kmp-pae-2.6_k3.16.7_45-24.1
vhba-kmp-pae-debuginfo-20140629_k3.16.7_45-2.22.1
pcfclock-kmp-pae-0.44_k3.16.7_45-260.22.1
crash-eppic-7.0.8-22.1
bbswitch-debugsource-0.8-3.22.1
cloop-debuginfo-2.639-14.22.1
cloop-kmp-desktop-debuginfo-2.639_k3.16.7_45-14.22.1
cloop-kmp-xen-debuginfo-2.639_k3.16.7_45-14.22.1
cloop-debugsource-2.639-14.22.1
xtables-addons-kmp-pae-debuginfo-2.6_k3.16.7_45-24.1
vhba-kmp-debugsource-20140629-2.22.1
crash-gcore-7.0.8-22.1
hdjmod-kmp-pae-1.28_k3.16.7_45-18.23.1
pcfclock-kmp-default-0.44_k3.16.7_45-260.22.1
hdjmod-debugsource-1.28-18.23.1
cloop-kmp-default-debuginfo-2.639_k3.16.7_45-14.22.1
ipset-kmp-default-6.23_k3.16.7_45-22.1
virtualbox-guest-kmp-default-5.0.28_k3.16.7_45-54.2
xtables-addons-debuginfo-2.6-24.1
bbswitch-kmp-desktop-0.8_k3.16.7_45-3.22.1
pcfclock-0.44-260.22.1

hdjmod-kmp-default-debuginfo-1.28_k3.16.7_45-18.23.1
virtualbox-guest-kmp-pae-5.0.28_k3.16.7_45-54.2
bbswitch-kmp-default-debuginfo-0.8_k3.16.7_45-3.22.1
ipset-kmp-xen-debuginfo-6.23_k3.16.7_45-22.1
bbswitch-kmp-xen-debuginfo-0.8_k3.16.7_45-3.22.1
kernel-obs-qa-3.16.7-45.1
xen-devel-4.4.4_05-51.2
ipset-debugsource-6.23-22.1
xtables-addons-2.6-24.1
crash-doc-7.0.8-22.1
xen-debugsource-4.4.4_05-51.2
vhba-kmp-desktop-20140629_k3.16.7_45-2.22.1
virtualbox-host-kmp-desktop-5.0.28_k3.16.7_45-54.2
kernel-obs-qa-xen-3.16.7-45.1
crash-kmp-xen-7.0.8_k3.16.7_45-22.1
virtualbox-5.0.28-54.2
pcfclock-debugsource-0.44-260.22.1
crash-7.0.8-22.1
crash-kmp-xen-debuginfo-7.0.8_k3.16.7_45-22.1
xen-tools-domU-debuginfo-4.4.4_05-51.2
virtualbox-debuginfo-5.0.28-54.2
xtables-addons-kmp-xen-2.6_k3.16.7_45-24.1
crash-kmp-pae-7.0.8_k3.16.7_45-22.1
virtualbox-debugsource-5.0.28-54.2
crash-kmp-default-7.0.8_k3.16.7_45-22.1
ipset-kmp-desktop-debuginfo-6.23_k3.16.7_45-22.1
virtualbox-qt-5.0.28-54.2
crash-kmp-desktop-debuginfo-7.0.8_k3.16.7_45-22.1
bbswitch-kmp-desktop-debuginfo-0.8_k3.16.7_45-3.22.1
kernel-default-debuginfo-3.16.7-45.1
bbswitch-kmp-xen-0.8_k3.16.7_45-3.22.1
crash-debugsource-7.0.8-22.1
cloop-2.639-14.22.1
xtables-addons-kmp-xen-debuginfo-2.6_k3.16.7_45-24.1
virtualbox-host-kmp-default-debuginfo-5.0.28_k3.16.7_45-54.2
kernel-default-base-debuginfo-3.16.7-45.1
pcfclock-kmp-default-debuginfo-0.44_k3.16.7_45-260.22.1
crash-kmp-default-debuginfo-7.0.8_k3.16.7_45-22.1
ipset-devel-6.23-22.1
virtualbox-guest-kmp-default-debuginfo-5.0.28_k3.16.7_45-54.2
hdjmod-kmp-xen-debuginfo-1.28_k3.16.7_45-18.23.1
vhba-kmp-xen-20140629_k3.16.7_45-2.22.1
xtables-addons-kmp-desktop-2.6_k3.16.7_45-24.1
hdjmod-kmp-default-1.28_k3.16.7_45-18.23.1
vhba-kmp-xen-debuginfo-20140629_k3.16.7_45-2.22.1
virtualbox-guest-kmp-desktop-debuginfo-5.0.28_k3.16.7_45-54.2
bbswitch-kmp-pae-0.8_k3.16.7_45-3.22.1
xtables-addons-kmp-default-2.6_k3.16.7_45-24.1
virtualbox-guest-x11-debuginfo-5.0.28-54.2
crash-kmp-desktop-7.0.8_k3.16.7_45-22.1

i686
kernel-debug-debuginfo-3.16.7-45.1
kernel-desktop-base-debuginfo-3.16.7-45.1
kernel-xen-devel-3.16.7-45.1
kernel-debug-devel-debuginfo-3.16.7-45.1
kernel-xen-debugsource-3.16.7-45.1
kernel-xen-base-debuginfo-3.16.7-45.1
kernel-debug-devel-3.16.7-45.1
kernel-ec2-base-debuginfo-3.16.7-45.1

kernel-vanilla-3.16.7-45.1
kernel-xen-base-3.16.7-45.1
kernel-debug-debugsource-3.16.7-45.1
kernel-desktop-debuginfo-3.16.7-45.1
kernel-debug-3.16.7-45.1
kernel-pae-base-3.16.7-45.1
kernel-desktop-debugsource-3.16.7-45.1
kernel-desktop-3.16.7-45.1
kernel-ec2-debuginfo-3.16.7-45.1
kernel-pae-devel-3.16.7-45.1
kernel-pae-debuginfo-3.16.7-45.1
kernel-debug-base-3.16.7-45.1
kernel-desktop-devel-3.16.7-45.1
kernel-vanilla-devel-3.16.7-45.1
kernel-vanilla-debuginfo-3.16.7-45.1
kernel-vanilla-debugsource-3.16.7-45.1
kernel-desktop-base-3.16.7-45.1
kernel-pae-base-debuginfo-3.16.7-45.1
kernel-debug-base-debuginfo-3.16.7-45.1
kernel-ec2-debugsource-3.16.7-45.1
kernel-pae-3.16.7-45.1
kernel-xen-debuginfo-3.16.7-45.1
kernel-xen-3.16.7-45.1
kernel-pae-debugsource-3.16.7-45.1

noarch
virtualbox-guest-desktop-icons-5.0.28-54.2
kernel-source-3.16.7-45.1
kernel-macros-3.16.7-45.1
kernel-docs-3.16.7-45.2
kernel-source-vanilla-3.16.7-45.1
kernel-devel-3.16.7-45.1
virtualbox-host-source-5.0.28-54.2

x86_64
virtualbox-guest-x11-5.0.28-54.2
crash-kmp-xen-7.0.8_k3.16.7_45-22.1
cloop-debuginfo-2.639-14.22.1
ipset-kmp-desktop-debuginfo-6.23_k3.16.7_45-22.1

182148 - FreeBSD flash Multiple Vulnerabilities (2482c798-93c6-11e6-846f-bc5ff4fb5ea1)

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

Risk Level: High

CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992

Description

The scan detected that the host is missing the following update:
flash -- multiple vulnerabilities (2482c798-93c6-11e6-846f-bc5ff4fb5ea1)

Observation

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

http://www.vuxml.org/freebsd/2482c798-93c6-11e6-846f-bc5ff4fb5ea1.html

Affected packages:

linux-c6-flashplugin < 11.2r202.637
linux-c6_64-flashplugin < 11.2r202.637
linux-c7-flashplugin < 11.2r202.637
linux-f10-flashplugin < 11.2r202.637

20736 - (JSA10759) Juniper Junos OpenSSL June to September 2016 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306, CVE-2016-6307, CVE-2016-6308, CVE-2016-6309, CVE-2016-7052

Description

Multiple vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper Junos. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition or to execute arbitrary remote code.

20742 - Cisco ASA Software Identity Firewall Feature Buffer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-6432

Description

A vulnerability is present in some versions of Cisco ASA Software.

Observation

Cisco ASA series of products provide Firewall and VPN functionality.

A vulnerability is present in some versions of Cisco ASA Software. The flaw lies in the Identity Firewall feature. Successful exploitation could allow an attacker to cause a reload of the affected system or to execute arbitrary code.

141307 - Red Hat Enterprise Linux RHSA-2016-2119 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7855

Description

The scan detected that the host is missing the following update:
RHSA-2016-2119

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2119.html

RHEL5S

x86_64
flash-plugin-11.2.202.643-1.el5_11

i386
flash-plugin-11.2.202.643-1.el5_11

RHEL6D
x86_64
flash-plugin-11.2.202.643-1.el6_8

i386
flash-plugin-11.2.202.643-1.el6_8

RHEL6S
x86_64
flash-plugin-11.2.202.643-1.el6_8

i386
flash-plugin-11.2.202.643-1.el6_8

RHEL6WS
x86_64
flash-plugin-11.2.202.643-1.el6_8

i386
flash-plugin-11.2.202.643-1.el6_8

RHEL5D
x86_64
flash-plugin-11.2.202.643-1.el5_11

i386
flash-plugin-11.2.202.643-1.el5_11

144952 - SuSE SLED 12 SP1 SUSE-SU-2016:2662-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7855

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2662-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002372.html

SuSE SLED 12 SP1
x86_64
flash-player-11.2.202.643-146.1
flash-player-gnome-11.2.202.643-146.1

20731 - Cisco NX-OS Software Malformed DHCPv4 Packet Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6393

Description

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the implementation of the DHCPv4 relay agent in Cisco NX-OS Software. Successful exploitation could allow an attacker to cause a denial of service condition.

20734 - Mozilla Firefox Multiple Vulnerabilities Prior To 49.0.2

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

Risk Level: High

CVE: CVE-2016-5287, CVE-2016-5288

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information from the HTTP cache or cause a denial of service condition.

20735 - Mozilla Firefox Multiple Vulnerabilities Prior To 49.0.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5287, CVE-2016-5288

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information from the HTTP cache or cause a denial of service condition.

130615 - Debian Linux 8.0 DSA-3700-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3008, CVE-2016-2232, CVE-2016-2316, CVE-2016-7551

Description

The scan detected that the host is missing the following update:
DSA-3700-1

Observation

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

http://www.debian.org/security/2016/dsa-3700

Debian 8.0
all
asterisk_1:11.13.1~dfsg-2+deb8u1

132288 - Oracle VM OVMSA-2016-0150 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0150

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000570.html

OVM3.3
x86_64
kernel-uek-3.8.13-118.13.3.el6uek
kernel-uek-firmware-3.8.13-118.13.3.el6uek

132291 - Oracle VM OVMSA-2016-0149 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0149

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000569.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-61.1.16.el6uek
kernel-uek-4.1.12-61.1.16.el6uek

141306 - Red Hat Enterprise Linux RHSA-2016-2105 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2105

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2105.html

RHEL6D
i386
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

noarch
kernel-firmware-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debuginfo-common-x86_64-2.6.32-642.6.2.el6

RHEL6S
i386
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6

kernel-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

noarch
kernel-firmware-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debuginfo-common-x86_64-2.6.32-642.6.2.el6

RHEL6WS
i386
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

noarch
kernel-firmware-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6

x86_64
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-debuginfo-common-x86_64-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

141308 - Red Hat Enterprise Linux RHSA-2016-2098 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2098

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2098.html

RHEL7D
x86_64
kernel-debug-devel-3.10.0-327.36.3.el7
python-perf-debuginfo-3.10.0-327.36.3.el7
perf-3.10.0-327.36.3.el7
kernel-tools-libs-3.10.0-327.36.3.el7
kernel-devel-3.10.0-327.36.3.el7
kernel-debug-3.10.0-327.36.3.el7
kernel-3.10.0-327.36.3.el7
kernel-debuginfo-common-x86_64-3.10.0-327.36.3.el7
python-perf-3.10.0-327.36.3.el7
kernel-tools-3.10.0-327.36.3.el7
perf-debuginfo-3.10.0-327.36.3.el7
kernel-debug-debuginfo-3.10.0-327.36.3.el7
kernel-debuginfo-3.10.0-327.36.3.el7
kernel-tools-libs-devel-3.10.0-327.36.3.el7
kernel-tools-debuginfo-3.10.0-327.36.3.el7
kernel-headers-3.10.0-327.36.3.el7

noarch
kernel-abi-whitelists-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7

RHEL7S
noarch
kernel-abi-whitelists-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7

RHEL7WS
x86_64
kernel-debug-devel-3.10.0-327.36.3.el7
python-perf-debuginfo-3.10.0-327.36.3.el7
perf-3.10.0-327.36.3.el7
kernel-tools-libs-3.10.0-327.36.3.el7
kernel-devel-3.10.0-327.36.3.el7
kernel-debug-3.10.0-327.36.3.el7
kernel-3.10.0-327.36.3.el7
kernel-debuginfo-common-x86_64-3.10.0-327.36.3.el7
python-perf-3.10.0-327.36.3.el7
kernel-tools-3.10.0-327.36.3.el7
perf-debuginfo-3.10.0-327.36.3.el7
kernel-debug-debuginfo-3.10.0-327.36.3.el7
kernel-debuginfo-3.10.0-327.36.3.el7
kernel-tools-libs-devel-3.10.0-327.36.3.el7
kernel-tools-debuginfo-3.10.0-327.36.3.el7

kernel-headers-3.10.0-327.36.3.el7

noarch
kernel-abi-whitelists-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7

141310 - Red Hat Enterprise Linux RHSA-2016-2099 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776, CVE-2016-2848

Description

The scan detected that the host is missing the following update:
RHSA-2016-2099

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2099.html

RHEL6_2S
x86_64
bind-sdb-9.7.3-8.P3.el6_2.5
bind-devel-9.7.3-8.P3.el6_2.5
bind-debuginfo-9.7.3-8.P3.el6_2.5

RHEL6_6S
i386
bind-libs-9.8.2-0.30.rc1.el6_6.6
bind-9.8.2-0.30.rc1.el6_6.6
bind-chroot-9.8.2-0.30.rc1.el6_6.6
bind-debuginfo-9.8.2-0.30.rc1.el6_6.6
bind-utils-9.8.2-0.30.rc1.el6_6.6

x86_64
bind-libs-9.8.2-0.30.rc1.el6_6.6
bind-9.8.2-0.30.rc1.el6_6.6
bind-chroot-9.8.2-0.30.rc1.el6_6.6
bind-debuginfo-9.8.2-0.30.rc1.el6_6.6
bind-utils-9.8.2-0.30.rc1.el6_6.6

141311 - Red Hat Enterprise Linux RHSA-2016-2124 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-5195

Description

The scan detected that the host is missing the following update:
RHSA-2016-2124

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2124.html

RHEL5D
i386
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5
kernel-PAE-devel-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-PAE-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-PAE-debuginfo-2.6.18-416.el5
kernel-headers-2.6.18-416.el5

noarch
kernel-doc-2.6.18-416.el5

x86_64
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5

RHEL5S
noarch
kernel-doc-2.6.18-416.el5

x86_64
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-xen-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-headers-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5

i386
kernel-2.6.18-416.el5
kernel-debuginfo-2.6.18-416.el5
kernel-PAE-devel-2.6.18-416.el5
kernel-debuginfo-common-2.6.18-416.el5
kernel-debug-debuginfo-2.6.18-416.el5
kernel-debug-2.6.18-416.el5
kernel-xen-2.6.18-416.el5

kernel-PAE-2.6.18-416.el5
kernel-devel-2.6.18-416.el5
kernel-xen-devel-2.6.18-416.el5
kernel-debug-devel-2.6.18-416.el5
kernel-xen-debuginfo-2.6.18-416.el5
kernel-PAE-debuginfo-2.6.18-416.el5
kernel-headers-2.6.18-416.el5

144942 - SuSE Linux 13.2 openSUSE-SU-2016:2607-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7568

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2607-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00085.html

SuSE Linux 13.2
x86_64
libgd3-32bit-2.1.0-7.19.1
gd-debugsource-2.1.0-7.19.1
libgd3-2.1.0-7.19.1
gd-debuginfo-2.1.0-7.19.1
gd-devel-2.1.0-7.19.1
libgd3-debuginfo-32bit-2.1.0-7.19.1
gd-2.1.0-7.19.1
libgd3-debuginfo-2.1.0-7.19.1

i586
gd-debugsource-2.1.0-7.19.1
libgd3-2.1.0-7.19.1
gd-debuginfo-2.1.0-7.19.1
gd-devel-2.1.0-7.19.1
gd-2.1.0-7.19.1
libgd3-debuginfo-2.1.0-7.19.1

144943 - SuSE Linux 13.2 openSUSE-SU-2016:2576-1 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:
openSUSE-SU-2016:2576-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00070.html

SuSE Linux 13.2
i586
libdbus-1-3-1.8.22-19.1
libdbus-1-3-debuginfo-1.8.22-19.1
dbus-1-debuginfo-1.8.22-19.1
dbus-1-devel-1.8.22-19.1
dbus-1-x11-debuginfo-1.8.22-19.1
dbus-1-x11-1.8.22-19.1
dbus-1-x11-debugsource-1.8.22-19.1
dbus-1-1.8.22-19.1
dbus-1-debugsource-1.8.22-19.1

noarch
dbus-1-devel-doc-1.8.22-19.1

x86_64
libdbus-1-3-1.8.22-19.1
dbus-1-debugsource-1.8.22-19.1
dbus-1-1.8.22-19.1
dbus-1-devel-32bit-1.8.22-19.1
libdbus-1-3-32bit-1.8.22-19.1
libdbus-1-3-debuginfo-32bit-1.8.22-19.1
dbus-1-x11-1.8.22-19.1
libdbus-1-3-debuginfo-1.8.22-19.1
dbus-1-debuginfo-32bit-1.8.22-19.1
dbus-1-x11-debugsource-1.8.22-19.1
dbus-1-debuginfo-1.8.22-19.1
dbus-1-devel-1.8.22-19.1
dbus-1-x11-debuginfo-1.8.22-19.1

144944 - SuSE Linux 13.2 openSUSE-SU-2016:2641-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8957, CVE-2015-8958, CVE-2016-5688, CVE-2016-6823, CVE-2016-7101, CVE-2016-7446, CVE-2016-7447, CVE-2016-7448, CVE-2016-7449, CVE-2016-7515, CVE-2016-7516, CVE-2016-7517, CVE-2016-7519, CVE-2016-7522, CVE-2016-7524, CVE-2016-7526, CVE-2016-7527, CVE-2016-7528, CVE-2016-7529, CVE-2016-7531, CVE-2016-7533, CVE-2016-7537, CVE-2016-7800, CVE-2016-7996, CVE-2016-7997, CVE-2016-8682, CVE-2016-8683, CVE-2016-8684

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2641-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00094.html

SuSE Linux 13.2
x86_64
libGraphicsMagick-Q16-3-debuginfo-1.3.20-12.1
GraphicsMagick-debuginfo-1.3.20-12.1
GraphicsMagick-1.3.20-12.1
libGraphicsMagickWand-Q16-2-1.3.20-12.1

libGraphicsMagick++-Q16-3-debuginfo-1.3.20-12.1
libGraphicsMagick-Q16-3-1.3.20-12.1
perl-GraphicsMagick-1.3.20-12.1
GraphicsMagick-debugsource-1.3.20-12.1
GraphicsMagick-devel-1.3.20-12.1
libGraphicsMagick3-config-1.3.20-12.1
perl-GraphicsMagick-debuginfo-1.3.20-12.1
libGraphicsMagick++-Q16-3-1.3.20-12.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-12.1
libGraphicsMagick++-devel-1.3.20-12.1

i586
libGraphicsMagick-Q16-3-debuginfo-1.3.20-12.1
GraphicsMagick-debuginfo-1.3.20-12.1
GraphicsMagick-1.3.20-12.1
libGraphicsMagickWand-Q16-2-1.3.20-12.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-12.1
libGraphicsMagick-Q16-3-1.3.20-12.1
perl-GraphicsMagick-1.3.20-12.1
GraphicsMagick-debugsource-1.3.20-12.1
GraphicsMagick-devel-1.3.20-12.1
libGraphicsMagick3-config-1.3.20-12.1
perl-GraphicsMagick-debuginfo-1.3.20-12.1
libGraphicsMagick++-Q16-3-1.3.20-12.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-12.1
libGraphicsMagick++-devel-1.3.20-12.1

144945 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2661-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4912, CVE-2016-7567

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2661-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002371.html

SuSE SLES 12 SP1
x86_64
openslp-32bit-2.0.0-17.1
openslp-server-2.0.0-17.1
openslp-debuginfo-2.0.0-17.1
openslp-debugsource-2.0.0-17.1
openslp-2.0.0-17.1
openslp-server-debuginfo-2.0.0-17.1
openslp-debuginfo-32bit-2.0.0-17.1

SuSE SLED 12 SP1
x86_64
openslp-debuginfo-32bit-2.0.0-17.1
openslp-2.0.0-17.1
openslp-32bit-2.0.0-17.1

openslp-debugsource-2.0.0-17.1
openslp-debuginfo-2.0.0-17.1

144946 - SuSE Linux 13.2 openSUSE-SU-2016:2617-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1245

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2617-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00089.html

SuSE Linux 13.2
x86_64
quagga-devel-0.99.23-2.12.1
quagga-0.99.23-2.12.1
quagga-debuginfo-0.99.23-2.12.1
quagga-debugsource-0.99.23-2.12.1

i586
quagga-devel-0.99.23-2.12.1
quagga-0.99.23-2.12.1
quagga-debuginfo-0.99.23-2.12.1
quagga-debugsource-0.99.23-2.12.1

144950 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2654-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8602

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2654-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002366.html

SuSE SLES 12 SP1
x86_64
ghostscript-x11-debuginfo-9.15-14.1
ghostscript-x11-9.15-14.1
ghostscript-debuginfo-9.15-14.1
ghostscript-debugsource-9.15-14.1
ghostscript-9.15-14.1

SuSE SLED 12 SP1
x86_64
ghostscript-x11-debuginfo-9.15-14.1
ghostscript-x11-9.15-14.1
ghostscript-debuginfo-9.15-14.1
ghostscript-debugsource-9.15-14.1
ghostscript-9.15-14.1

144951 - SuSE Linux 13.2 openSUSE-SU-2016:2648-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-5653, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2648-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00101.html

SuSE Linux 13.2
x86_64
ghostscript-mini-debugsource-9.15-6.1
ghostscript-mini-devel-9.15-6.1
ghostscript-x11-9.15-6.1
ghostscript-debugsource-9.15-6.1
ghostscript-9.15-6.1
ghostscript-mini-debuginfo-9.15-6.1
ghostscript-debuginfo-9.15-6.1
ghostscript-devel-9.15-6.1
ghostscript-x11-debuginfo-9.15-6.1
ghostscript-mini-9.15-6.1

i586
ghostscript-mini-debugsource-9.15-6.1
ghostscript-mini-devel-9.15-6.1
ghostscript-x11-9.15-6.1
ghostscript-debugsource-9.15-6.1
ghostscript-9.15-6.1
ghostscript-mini-debuginfo-9.15-6.1
ghostscript-debuginfo-9.15-6.1
ghostscript-devel-9.15-6.1
ghostscript-x11-debuginfo-9.15-6.1
ghostscript-mini-9.15-6.1

144953 - SuSE Linux 13.2 openSUSE-SU-2016:2597-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2597-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00076.html

SuSE Linux 13.2
x86_64
chromium-debuginfo-54.0.2840.59-131.2
chromium-54.0.2840.59-131.2
chromium-ffmpegsumo-debuginfo-54.0.2840.59-131.2
chromium-ffmpegsumo-54.0.2840.59-131.2
chromedriver-54.0.2840.59-131.2
chromium-debugsource-54.0.2840.59-131.2
chromedriver-debuginfo-54.0.2840.59-131.2

i586
chromium-debuginfo-54.0.2840.59-131.2
chromium-54.0.2840.59-131.2
chromium-ffmpegsumo-debuginfo-54.0.2840.59-131.2
chromium-ffmpegsumo-54.0.2840.59-131.2
chromedriver-54.0.2840.59-131.2
chromium-debugsource-54.0.2840.59-131.2
chromedriver-debuginfo-54.0.2840.59-131.2

144957 - SuSE Linux 13.2 openSUSE-SU-2016:2606-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-7568, CVE-2016-8670

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2606-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00084.html

SuSE Linux 13.2
i586
php5-dom-debuginfo-5.6.1-83.1
php5-xsl-5.6.1-83.1
php5-dom-5.6.1-83.1
php5-iconv-debuginfo-5.6.1-83.1
php5-gmp-debuginfo-5.6.1-83.1
php5-tokenizer-5.6.1-83.1
php5-openssl-5.6.1-83.1
php5-readline-debuginfo-5.6.1-83.1
php5-iconv-5.6.1-83.1
php5-wddx-5.6.1-83.1
php5-suhosin-debuginfo-5.6.1-83.1

php5-wddx-debuginfo-5.6.1-83.1
php5-xmlwriter-debuginfo-5.6.1-83.1
php5-enchant-debuginfo-5.6.1-83.1
php5-fileinfo-5.6.1-83.1
php5-mysql-5.6.1-83.1
php5-bcmath-debuginfo-5.6.1-83.1
php5-calendar-debuginfo-5.6.1-83.1
php5-sysvshm-debuginfo-5.6.1-83.1
php5-ftp-5.6.1-83.1
php5-tidy-debuginfo-5.6.1-83.1
php5-exif-5.6.1-83.1
php5-pcntl-debuginfo-5.6.1-83.1
php5-fpm-debuginfo-5.6.1-83.1
php5-posix-debuginfo-5.6.1-83.1
php5-posix-5.6.1-83.1
php5-json-debuginfo-5.6.1-83.1
php5-zip-debuginfo-5.6.1-83.1
php5-opcache-5.6.1-83.1
php5-phar-5.6.1-83.1
php5-zlib-debuginfo-5.6.1-83.1
php5-curl-5.6.1-83.1
php5-fastcgi-debuginfo-5.6.1-83.1
php5-snmp-debuginfo-5.6.1-83.1
php5-suhosin-5.6.1-83.1
php5-sockets-5.6.1-83.1
php5-mssql-debuginfo-5.6.1-83.1
php5-sysvsem-5.6.1-83.1
php5-readline-5.6.1-83.1
php5-imap-debuginfo-5.6.1-83.1
php5-mbstring-debuginfo-5.6.1-83.1
php5-fileinfo-debuginfo-5.6.1-83.1
php5-sysvmsg-5.6.1-83.1
php5-calendar-5.6.1-83.1
php5-bcmath-5.6.1-83.1
php5-pdo-5.6.1-83.1
php5-openssl-debuginfo-5.6.1-83.1
php5-tidy-5.6.1-83.1
php5-soap-5.6.1-83.1
php5-debugsource-5.6.1-83.1
php5-pcntl-5.6.1-83.1
php5-bz2-debuginfo-5.6.1-83.1
php5-zlib-5.6.1-83.1
php5-debuginfo-5.6.1-83.1
php5-odbc-debuginfo-5.6.1-83.1
php5-soap-debuginfo-5.6.1-83.1
php5-zip-5.6.1-83.1
apache2-mod_php5-5.6.1-83.1
php5-sysvmsg-debuginfo-5.6.1-83.1
php5-bz2-5.6.1-83.1
php5-ftp-debuginfo-5.6.1-83.1
php5-shmop-5.6.1-83.1
php5-gmp-5.6.1-83.1
php5-dba-5.6.1-83.1
php5-gd-5.6.1-83.1
php5-devel-5.6.1-83.1
php5-ldap-debuginfo-5.6.1-83.1
php5-shmop-debuginfo-5.6.1-83.1
php5-xmlrpc-5.6.1-83.1
php5-firebird-debuginfo-5.6.1-83.1
php5-xmlwriter-5.6.1-83.1

php5-enchant-5.6.1-83.1
php5-sockets-debuginfo-5.6.1-83.1
php5-sqlite-debuginfo-5.6.1-83.1
php5-fastcgi-5.6.1-83.1
php5-json-5.6.1-83.1
php5-tokenizer-debuginfo-5.6.1-83.1
php5-5.6.1-83.1
apache2-mod_php5-debuginfo-5.6.1-83.1
php5-sysvshm-5.6.1-83.1
php5-intl-debuginfo-5.6.1-83.1
php5-ctype-debuginfo-5.6.1-83.1
php5-xmlreader-debuginfo-5.6.1-83.1
php5-sqlite-5.6.1-83.1
php5-phar-debuginfo-5.6.1-83.1
php5-xsl-debuginfo-5.6.1-83.1
php5-exif-debuginfo-5.6.1-83.1
php5-mcrypt-debuginfo-5.6.1-83.1
php5-snmp-5.6.1-83.1
php5-imap-5.6.1-83.1
php5-mcrypt-5.6.1-83.1
php5-xmlreader-5.6.1-83.1
php5-dba-debuginfo-5.6.1-83.1
php5-gettext-debuginfo-5.6.1-83.1
php5-fpm-5.6.1-83.1
php5-opcache-debuginfo-5.6.1-83.1
php5-mssql-5.6.1-83.1
php5-pdo-debuginfo-5.6.1-83.1
php5-odbc-5.6.1-83.1
php5-curl-debuginfo-5.6.1-83.1
php5-gd-debuginfo-5.6.1-83.1
php5-mbstring-5.6.1-83.1
php5-xmlrpc-debuginfo-5.6.1-83.1
php5-ctype-5.6.1-83.1
php5-gettext-5.6.1-83.1
php5-sysvsem-debuginfo-5.6.1-83.1
php5-ldap-5.6.1-83.1
php5-pgsql-debuginfo-5.6.1-83.1
php5-firebird-5.6.1-83.1
php5-pspell-5.6.1-83.1
php5-pspell-debuginfo-5.6.1-83.1
php5-mysql-debuginfo-5.6.1-83.1
php5-intl-5.6.1-83.1
php5-pgsql-5.6.1-83.1

noarch
php5-pear-5.6.1-83.1

x86_64
php5-dom-debuginfo-5.6.1-83.1
php5-xsl-5.6.1-83.1
php5-dom-5.6.1-83.1
php5-iconv-debuginfo-5.6.1-83.1
php5-gmp-debuginfo-5.6.1-83.1
php5-tokenizer-5.6.1-83.1
php5-openssl-5.6.1-83.1
php5-readline-debuginfo-5.6.1-83.1
php5-iconv-5.6.1-83.1
php5-wddx-5.6.1-83.1
php5-suhosin-debuginfo-5.6.1-83.1
php5-wddx-debuginfo-5.6.1-83.1

php5-xmlwriter-debuginfo-5.6.1-83.1
php5-enchant-debuginfo-5.6.1-83.1
php5-fileinfo-5.6.1-83.1
php5-mysql-5.6.1-83.1
php5-bcmath-debuginfo-5.6.1-83.1
php5-calendar-debuginfo-5.6.1-83.1
php5-sysvshm-debuginfo-5.6.1-83.1
php5-ftp-5.6.1-83.1
php5-tidy-debuginfo-5.6.1-83.1
php5-exif-5.6.1-83.1
php5-pcntl-debuginfo-5.6.1-83.1
php5-fpm-debuginfo-5.6.1-83.1
php5-posix-debuginfo-5.6.1-83.1
php5-posix-5.6.1-83.1
php5-json-debuginfo-5.6.1-83.1
php5-zip-debuginfo-5.6.1-83.1
php5-opcache-5.6.1-83.1
php5-phar-5.6.1-83.1
php5-zlib-debuginfo-5.6.1-83.1
php5-curl-5.6.1-83.1
php5-fastcgi-debuginfo-5.6.1-83.1
php5-snmp-debuginfo-5.6.1-83.1
php5-suhosin-5.6.1-83.1
php5-sockets-5.6.1-83.1
php5-mssql-debuginfo-5.6.1-83.1
php5-sysvsem-5.6.1-83.1
php5-readline-5.6.1-83.1
php5-imap-debuginfo-5.6.1-83.1
php5-mbstring-debuginfo-5.6.1-83.1
php5-fileinfo-debuginfo-5.6.1-83.1
php5-sysvmsg-5.6.1-83.1
php5-calendar-5.6.1-83.1
php5-bcmath-5.6.1-83.1
php5-pdo-5.6.1-83.1
php5-openssl-debuginfo-5.6.1-83.1
php5-tidy-5.6.1-83.1
php5-soap-5.6.1-83.1
php5-debugsource-5.6.1-83.1
php5-pcntl-5.6.1-83.1
php5-bz2-debuginfo-5.6.1-83.1
php5-zlib-5.6.1-83.1
php5-debuginfo-5.6.1-83.1
php5-odbc-debuginfo-5.6.1-83.1
php5-soap-debuginfo-5.6.1-83.1
php5-zip-5.6.1-83.1
apache2-mod_php5-5.6.1-83.1
php5-sysvmsg-debuginfo-5.6.1-83.1
php5-bz2-5.6.1-83.1
php5-ftp-debuginfo-5.6.1-83.1
php5-shmop-5.6.1-83.1
php5-gmp-5.6.1-83.1
php5-dba-5.6.1-83.1
php5-gd-5.6.1-83.1
php5-devel-5.6.1-83.1
php5-ldap-debuginfo-5.6.1-83.1
php5-shmop-debuginfo-5.6.1-83.1
php5-xmlrpc-5.6.1-83.1
php5-firebird-debuginfo-5.6.1-83.1
php5-xmlwriter-5.6.1-83.1
php5-enchant-5.6.1-83.1

php5-sockets-debuginfo-5.6.1-83.1
php5-sqlite-debuginfo-5.6.1-83.1
php5-fastcgi-5.6.1-83.1
php5-json-5.6.1-83.1
php5-tokenizer-debuginfo-5.6.1-83.1
php5-5.6.1-83.1
apache2-mod_php5-debuginfo-5.6.1-83.1
php5-sysvshm-5.6.1-83.1
php5-intl-debuginfo-5.6.1-83.1
php5-ctype-debuginfo-5.6.1-83.1
php5-xmlreader-debuginfo-5.6.1-83.1
php5-sqlite-5.6.1-83.1
php5-phar-debuginfo-5.6.1-83.1
php5-xsl-debuginfo-5.6.1-83.1
php5-exif-debuginfo-5.6.1-83.1
php5-mcrypt-debuginfo-5.6.1-83.1
php5-snmp-5.6.1-83.1
php5-imap-5.6.1-83.1
php5-mcrypt-5.6.1-83.1
php5-xmlreader-5.6.1-83.1
php5-dba-debuginfo-5.6.1-83.1
php5-gettext-debuginfo-5.6.1-83.1
php5-fpm-5.6.1-83.1
php5-opcache-debuginfo-5.6.1-83.1
php5-mssql-5.6.1-83.1
php5-pdo-debuginfo-5.6.1-83.1
php5-odbc-5.6.1-83.1
php5-curl-debuginfo-5.6.1-83.1
php5-gd-debuginfo-5.6.1-83.1
php5-mbstring-5.6.1-83.1
php5-xmlrpc-debuginfo-5.6.1-83.1
php5-ctype-5.6.1-83.1
php5-gettext-5.6.1-83.1
php5-sysvsem-debuginfo-5.6.1-83.1
php5-ldap-5.6.1-83.1
php5-pgsql-debuginfo-5.6.1-83.1
php5-firebird-5.6.1-83.1
php5-pspell-5.6.1-83.1
php5-pspell-debuginfo-5.6.1-83.1
php5-mysql-debuginfo-5.6.1-83.1
php5-intl-5.6.1-83.1
php5-pgsql-5.6.1-83.1

144958 - SuSE Linux 13.2 openSUSE-SU-2016:2603-1 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:
openSUSE-SU-2016:2603-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00081.html

SuSE Linux 13.2
x86_64
tor-0.2.7.6-26.1
tor-debugsource-0.2.7.6-26.1
tor-debuginfo-0.2.7.6-26.1

i586
tor-0.2.7.6-26.1
tor-debugsource-0.2.7.6-26.1
tor-debuginfo-0.2.7.6-26.1

144959 - SuSE Linux 13.1 openSUSE-SU-2016:2584-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195, CVE-2016-8666

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2584-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00075.html

SuSE Linux 13.1
i586
iscsitarget-kmp-desktop-debuginfo-1.4.20.3_k3.12.62_55-13.34.1
virtualbox-guest-kmp-desktop-4.2.36_k3.12.62_55-2.66.1
openvswitch-test-1.11.0-0.41.1
ndiswrapper-debugsource-1.58-35.1
openvswitch-pki-1.11.0-0.41.1
iscsitarget-kmp-default-1.4.20.3_k3.12.62_55-13.34.1
pcfclock-0.44-258.35.1
xen-devel-4.3.4_10-67.1
openvswitch-kmp-default-debuginfo-1.11.0_k3.12.62_55-0.41.1
ipset-kmp-desktop-debuginfo-6.21.1_k3.12.62_55-2.38.1
xtables-addons-kmp-default-debuginfo-2.3_k3.12.62_55-2.33.1
hdjmod-kmp-pae-1.28_k3.12.62_55-16.34.1
xen-libs-4.3.4_10-67.1
hdjmod-kmp-default-1.28_k3.12.62_55-16.34.1
iscsitarget-kmp-pae-debuginfo-1.4.20.3_k3.12.62_55-13.34.1
xen-kmp-default-debuginfo-4.3.4_10_k3.12.62_55-67.1
openvswitch-1.11.0-0.41.1
ndiswrapper-kmp-desktop-debuginfo-1.58_k3.12.62_55-35.1
virtualbox-guest-x11-debuginfo-4.2.36-2.66.1
ndiswrapper-kmp-pae-1.58_k3.12.62_55-35.1
ipset-kmp-default-6.21.1_k3.12.62_55-2.38.1
iscsitarget-kmp-pae-1.4.20.3_k3.12.62_55-13.34.1
crash-devel-7.0.2-2.34.1
xen-kmp-default-4.3.4_10_k3.12.62_55-67.1
virtualbox-host-kmp-pae-debuginfo-4.2.36_k3.12.62_55-2.66.1
pcfclock-kmp-desktop-debuginfo-0.44_k3.12.62_55-258.35.1
iscsitarget-debuginfo-1.4.20.3-13.34.1
vhba-kmp-xen-20130607_k3.12.62_55-2.34.1
xtables-addons-kmp-desktop-debuginfo-2.3_k3.12.62_55-2.33.1

hdjmod-kmp-desktop-1.28_k3.12.62_55-16.34.1
virtualbox-4.2.36-2.66.1
hdjmod-kmp-xen-debuginfo-1.28_k3.12.62_55-16.34.1
openvswitch-kmp-desktop-1.11.0_k3.12.62_55-0.41.1
xtables-addons-kmp-xen-2.3_k3.12.62_55-2.33.1
vhba-kmp-default-20130607_k3.12.62_55-2.34.1
openvswitch-kmp-pae-1.11.0_k3.12.62_55-0.41.1
cloop-kmp-desktop-debuginfo-2.639_k3.12.62_55-11.34.1
openvswitch-debugsource-1.11.0-0.41.1
cloop-kmp-default-2.639_k3.12.62_55-11.34.1
virtualbox-host-kmp-desktop-debuginfo-4.2.36_k3.12.62_55-2.66.1
ndiswrapper-kmp-default-1.58_k3.12.62_55-35.1
kernel-default-3.12.62-55.1
ndiswrapper-debuginfo-1.58-35.1
iscsitarget-1.4.20.3-13.34.1
hdjmod-kmp-default-debuginfo-1.28_k3.12.62_55-16.34.1
vhba-kmp-pae-20130607_k3.12.62_55-2.34.1
virtualbox-websrv-debuginfo-4.2.36-2.66.1
pcfclock-kmp-desktop-0.44_k3.12.62_55-258.35.1
python-virtualbox-4.2.36-2.66.1
virtualbox-host-kmp-default-debuginfo-4.2.36_k3.12.62_55-2.66.1
xen-kmp-desktop-4.3.4_10_k3.12.62_55-67.1
virtualbox-guest-kmp-default-debuginfo-4.2.36_k3.12.62_55-2.66.1
virtualbox-websrv-4.2.36-2.66.1
xen-libs-debuginfo-4.3.4_10-67.1
virtualbox-guest-x11-4.2.36-2.66.1
crash-gcore-7.0.2-2.34.1
xtables-addons-kmp-desktop-2.3_k3.12.62_55-2.33.1
kernel-default-base-debuginfo-3.12.62-55.1
pcfclock-debugsource-0.44-258.35.1
openvswitch-kmp-xen-1.11.0_k3.12.62_55-0.41.1
virtualbox-qt-debuginfo-4.2.36-2.66.1
iscsitarget-debugsource-1.4.20.3-13.34.1
iscsitarget-kmp-default-debuginfo-1.4.20.3_k3.12.62_55-13.34.1
virtualbox-guest-kmp-pae-debuginfo-4.2.36_k3.12.62_55-2.66.1
xtables-addons-kmp-xen-debuginfo-2.3_k3.12.62_55-2.33.1
xtables-addons-2.3-2.33.1
libipset3-debuginfo-6.21.1-2.38.1
vhba-kmp-xen-debuginfo-20130607_k3.12.62_55-2.34.1
openvswitch-switch-debuginfo-1.11.0-0.41.1
crash-doc-7.0.2-2.34.1
ipset-kmp-xen-6.21.1_k3.12.62_55-2.38.1
ndiswrapper-kmp-desktop-1.58_k3.12.62_55-35.1
libipset3-6.21.1-2.38.1
ipset-kmp-default-debuginfo-6.21.1_k3.12.62_55-2.38.1
hdjmod-kmp-desktop-debuginfo-1.28_k3.12.62_55-16.34.1
vhba-kmp-desktop-20130607_k3.12.62_55-2.34.1
crash-kmp-xen-7.0.2_k3.12.62_55-2.34.1
crash-kmp-default-7.0.2_k3.12.62_55-2.34.1
ipset-debugsource-6.21.1-2.38.1
iscsitarget-kmp-xen-debuginfo-1.4.20.3_k3.12.62_55-13.34.1
cloop-kmp-default-debuginfo-2.639_k3.12.62_55-11.34.1
crash-kmp-desktop-debuginfo-7.0.2_k3.12.62_55-2.34.1
cloop-kmp-xen-debuginfo-2.639_k3.12.62_55-11.34.1
openvswitch-kmp-desktop-debuginfo-1.11.0_k3.12.62_55-0.41.1
xtables-addons-kmp-pae-debuginfo-2.3_k3.12.62_55-2.33.1
ndiswrapper-kmp-default-debuginfo-1.58_k3.12.62_55-35.1
cloop-kmp-xen-2.639_k3.12.62_55-11.34.1
openvswitch-controller-debuginfo-1.11.0-0.41.1
virtualbox-host-kmp-pae-4.2.36_k3.12.62_55-2.66.1

python-openvswitch-test-1.11.0-0.41.1
openvswitch-kmp-xen-debuginfo-1.11.0_k3.12.62_55-0.41.1
openvswitch-kmp-pae-debuginfo-1.11.0_k3.12.62_55-0.41.1
crash-debuginfo-7.0.2-2.34.1
vhba-kmp-desktop-debuginfo-20130607_k3.12.62_55-2.34.1
crash-eppic-debuginfo-7.0.2-2.34.1
kernel-default-base-3.12.62-55.1
crash-kmp-default-debuginfo-7.0.2_k3.12.62_55-2.34.1
ndiswrapper-kmp-pae-debuginfo-1.58_k3.12.62_55-35.1
pcfclock-kmp-default-debuginfo-0.44_k3.12.62_55-258.35.1
xen-tools-domU-debuginfo-4.3.4_10-67.1
ndiswrapper-1.58-35.1
hdjmod-kmp-pae-debuginfo-1.28_k3.12.62_55-16.34.1
virtualbox-guest-kmp-default-4.2.36_k3.12.62_55-2.66.1
virtualbox-host-kmp-desktop-4.2.36_k3.12.62_55-2.66.1
crash-gcore-debuginfo-7.0.2-2.34.1
virtualbox-guest-kmp-pae-4.2.36_k3.12.62_55-2.66.1
pcfclock-kmp-pae-debuginfo-0.44_k3.12.62_55-258.35.1
vhba-kmp-default-debuginfo-20130607_k3.12.62_55-2.34.1
kernel-default-debuginfo-3.12.62-55.1
pcfclock-kmp-pae-0.44_k3.12.62_55-258.35.1
cloop-debugsource-2.639-11.34.1
xtables-addons-debuginfo-2.3-2.33.1
crash-kmp-desktop-7.0.2_k3.12.62_55-2.34.1
cloop-kmp-pae-2.639_k3.12.62_55-11.34.1
pcfclock-debuginfo-0.44-258.35.1
ipset-kmp-pae-6.21.1_k3.12.62_55-2.38.1
hdjmod-debugsource-1.28-16.34.1
crash-7.0.2-2.34.1
crash-kmp-xen-debuginfo-7.0.2_k3.12.62_55-2.34.1
crash-debugsource-7.0.2-2.34.1
openvswitch-debuginfo-1.11.0-0.41.1
iscsitarget-kmp-xen-1.4.20.3_k3.12.62_55-13.34.1
virtualbox-devel-4.2.36-2.66.1
xen-tools-domU-4.3.4_10-67.1
virtualbox-debugsource-4.2.36-2.66.1
crash-eppic-7.0.2-2.34.1
ipset-6.21.1-2.38.1
hdjmod-kmp-xen-1.28_k3.12.62_55-16.34.1
ipset-kmp-xen-debuginfo-6.21.1_k3.12.62_55-2.38.1
kernel-default-debugsource-3.12.62-55.1
openvswitch-controller-1.11.0-0.41.1
crash-kmp-pae-7.0.2_k3.12.62_55-2.34.1
virtualbox-debuginfo-4.2.36-2.66.1
ipset-kmp-desktop-6.21.1_k3.12.62_55-2.38.1
openvswitch-kmp-default-1.11.0_k3.12.62_55-0.41.1
vhba-kmp-pae-debuginfo-20130607_k3.12.62_55-2.34.1
cloop-2.639-11.34.1
cloop-kmp-pae-debuginfo-2.639_k3.12.62_55-11.34.1
xen-kmp-desktop-debuginfo-4.3.4_10_k3.12.62_55-67.1
ipset-kmp-pae-debuginfo-6.21.1_k3.12.62_55-2.38.1
cloop-debuginfo-2.639-11.34.1
virtualbox-guest-tools-debuginfo-4.2.36-2.66.1
ipset-devel-6.21.1-2.38.1
kernel-default-devel-3.12.62-55.1
iscsitarget-kmp-desktop-1.4.20.3_k3.12.62_55-13.34.1
xtables-addons-debugsource-2.3-2.33.1
xen-debugsource-4.3.4_10-67.1
vhba-kmp-debugsource-20130607-2.34.1
virtualbox-guest-kmp-desktop-debuginfo-4.2.36_k3.12.62_55-2.66.1

xtables-addons-kmp-default-2.3_k3.12.62_55-2.33.1
ipset-debuginfo-6.21.1-2.38.1
virtualbox-host-kmp-default-4.2.36_k3.12.62_55-2.66.1
openvswitch-switch-1.11.0-0.41.1
kernel-syms-3.12.62-55.1
python-openvswitch-1.11.0-0.41.1
virtualbox-qt-4.2.36-2.66.1
xen-kmp-pae-4.3.4_10_k3.12.62_55-67.1
xen-kmp-pae-debuginfo-4.3.4_10_k3.12.62_55-67.1
xtables-addons-kmp-pae-2.3_k3.12.62_55-2.33.1
python-virtualbox-debuginfo-4.2.36-2.66.1

144960 - SuSE Linux 13.2 openSUSE-SU-2016:2623-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5501, CVE-2016-5538, CVE-2016-5605, CVE-2016-5608, CVE-2016-5610, CVE-2016-5611, CVE-2016-5613

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2623-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00090.html

SuSE Linux 13.2
i586
virtualbox-debuginfo-5.0.28-54.1
virtualbox-host-kmp-desktop-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-kmp-pae-5.0.28_k3.16.7_42-54.1
virtualbox-host-kmp-default-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-kmp-default-5.0.28_k3.16.7_42-54.1
virtualbox-guest-kmp-desktop-5.0.28_k3.16.7_42-54.1
virtualbox-host-kmp-default-5.0.28_k3.16.7_42-54.1
virtualbox-qt-debuginfo-5.0.28-54.1
virtualbox-host-kmp-pae-5.0.28_k3.16.7_42-54.1
virtualbox-guest-tools-5.0.28-54.1
virtualbox-5.0.28-54.1
virtualbox-debugsource-5.0.28-54.1
virtualbox-guest-kmp-desktop-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-tools-debuginfo-5.0.28-54.1
virtualbox-devel-5.0.28-54.1
virtualbox-websrv-5.0.28-54.1
virtualbox-qt-5.0.28-54.1
virtualbox-guest-kmp-default-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-x11-debuginfo-5.0.28-54.1
virtualbox-websrv-debuginfo-5.0.28-54.1
virtualbox-host-kmp-pae-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-host-kmp-desktop-5.0.28_k3.16.7_42-54.1
python-virtualbox-5.0.28-54.1
python-virtualbox-debuginfo-5.0.28-54.1
virtualbox-guest-kmp-pae-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-x11-5.0.28-54.1

noarch

virtualbox-guest-desktop-icons-5.0.28-54.1
virtualbox-host-source-5.0.28-54.1

x86_64
virtualbox-debuginfo-5.0.28-54.1
virtualbox-host-kmp-desktop-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-host-kmp-default-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-kmp-default-5.0.28_k3.16.7_42-54.1
virtualbox-guest-kmp-desktop-5.0.28_k3.16.7_42-54.1
virtualbox-host-kmp-default-5.0.28_k3.16.7_42-54.1
virtualbox-qt-debuginfo-5.0.28-54.1
virtualbox-guest-tools-5.0.28-54.1
virtualbox-5.0.28-54.1
virtualbox-debugsource-5.0.28-54.1
virtualbox-guest-kmp-desktop-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-tools-debuginfo-5.0.28-54.1
virtualbox-devel-5.0.28-54.1
virtualbox-websrv-5.0.28-54.1
virtualbox-qt-5.0.28-54.1
virtualbox-guest-kmp-default-debuginfo-5.0.28_k3.16.7_42-54.1
virtualbox-guest-x11-debuginfo-5.0.28-54.1
virtualbox-websrv-debuginfo-5.0.28-54.1
virtualbox-host-kmp-desktop-5.0.28_k3.16.7_42-54.1
python-virtualbox-5.0.28-54.1
python-virtualbox-debuginfo-5.0.28-54.1
virtualbox-guest-x11-5.0.28-54.1

144962 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2592-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2592-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002345.html

SuSE SLES 12 SP1
noarch
kernel-devel-3.12.62-60.64.8.2
kernel-source-3.12.62-60.64.8.2
kernel-macros-3.12.62-60.64.8.2

x86_64
kernel-xen-base-debuginfo-3.12.62-60.64.8.2
kernel-xen-debugsource-3.12.62-60.64.8.2
kernel-default-3.12.62-60.64.8.2
kernel-default-devel-3.12.62-60.64.8.2
kernel-default-debugsource-3.12.62-60.64.8.2
kernel-syms-3.12.62-60.64.8.2
kernel-xen-debuginfo-3.12.62-60.64.8.2
kernel-xen-devel-3.12.62-60.64.8.2

kernel-xen-3.12.62-60.64.8.2
kernel-default-base-3.12.62-60.64.8.2
kernel-default-debuginfo-3.12.62-60.64.8.2
kernel-default-base-debuginfo-3.12.62-60.64.8.2
kernel-xen-base-3.12.62-60.64.8.2

SuSE SLED 12 SP1
x86_64
kernel-syms-3.12.62-60.64.8.2
kernel-default-extra-3.12.62-60.64.8.2
kernel-default-debuginfo-3.12.62-60.64.8.2
kernel-xen-devel-3.12.62-60.64.8.2
kernel-xen-debuginfo-3.12.62-60.64.8.2
kernel-xen-debugsource-3.12.62-60.64.8.2
kernel-default-debugsource-3.12.62-60.64.8.2
kernel-default-devel-3.12.62-60.64.8.2
kernel-default-3.12.62-60.64.8.2
kernel-xen-3.12.62-60.64.8.2
kernel-default-extra-debuginfo-3.12.62-60.64.8.2

noarch
kernel-devel-3.12.62-60.64.8.2
kernel-source-3.12.62-60.64.8.2
kernel-macros-3.12.62-60.64.8.2

144964 - SuSE Linux 13.2 openSUSE-SU-2016:2639-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5287, CVE-2016-5288

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2639-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00092.html

SuSE Linux 13.2
x86_64
MozillaFirefox-debuginfo-49.0.2-84.1
MozillaFirefox-debugsource-49.0.2-84.1
MozillaFirefox-branding-upstream-49.0.2-84.1
MozillaFirefox-buildsymbols-49.0.2-84.1
MozillaFirefox-49.0.2-84.1
MozillaFirefox-translations-other-49.0.2-84.1
MozillaFirefox-translations-common-49.0.2-84.1
MozillaFirefox-devel-49.0.2-84.1

i586
MozillaFirefox-branding-upstream-49.0.2-84.1
MozillaFirefox-buildsymbols-49.0.2-84.1
MozillaFirefox-49.0.2-84.1
MozillaFirefox-translations-other-49.0.2-84.1
MozillaFirefox-translations-common-49.0.2-84.1

MozillaFirefox-devel-49.0.2-84.1

144965 - SuSE SLES 12 SP1 SUSE-SU-2016:2618-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1245

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2618-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002350.html

SuSE SLES 12 SP1
x86_64
quagga-0.99.22.1-15.1
quagga-debuginfo-0.99.22.1-15.1
quagga-debugsource-0.99.22.1-15.1

144967 - SuSE SLES 11 SP4 SUSE-SU-2016:2585-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2585-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002343.html

SuSE SLES 11 SP4
i586
kernel-ec2-3.0.101-84.1
kernel-pae-base-3.0.101-84.1
kernel-xen-3.0.101-84.1
kernel-trace-3.0.101-84.1
kernel-pae-devel-3.0.101-84.1
kernel-xen-base-3.0.101-84.1
kernel-pae-3.0.101-84.1
kernel-syms-3.0.101-84.1
kernel-trace-devel-3.0.101-84.1
kernel-default-devel-3.0.101-84.1
kernel-source-3.0.101-84.1
kernel-ec2-devel-3.0.101-84.1
kernel-xen-devel-3.0.101-84.1
kernel-default-3.0.101-84.1

kernel-default-base-3.0.101-84.1
kernel-trace-base-3.0.101-84.1
kernel-ec2-base-3.0.101-84.1

x86_64
kernel-ec2-3.0.101-84.1
kernel-xen-3.0.101-84.1
kernel-trace-3.0.101-84.1
kernel-xen-base-3.0.101-84.1
kernel-syms-3.0.101-84.1
kernel-trace-devel-3.0.101-84.1
kernel-default-devel-3.0.101-84.1
kernel-source-3.0.101-84.1
kernel-ec2-devel-3.0.101-84.1
kernel-xen-devel-3.0.101-84.1
kernel-default-3.0.101-84.1
kernel-default-base-3.0.101-84.1
kernel-trace-base-3.0.101-84.1
kernel-ec2-base-3.0.101-84.1

160158 - CentOS 6 CESA-2016-2105 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
CESA-2016-2105

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-October/022134.html

CentOS 6
i686
kernel-debug-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

noarch
kernel-firmware-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6

x86_64
kernel-debug-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6

perf-2.6.32-642.6.2.el6

160159 - CentOS 7 CESA-2016-2098 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
CESA-2016-2098

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-October/022133.html

CentOS 7
x86_64
kernel-tools-libs-devel-3.10.0-327.36.3.el7
kernel-tools-3.10.0-327.36.3.el7
kernel-headers-3.10.0-327.36.3.el7
python-perf-3.10.0-327.36.3.el7
kernel-3.10.0-327.36.3.el7
kernel-debug-devel-3.10.0-327.36.3.el7
perf-3.10.0-327.36.3.el7
kernel-debug-3.10.0-327.36.3.el7
kernel-devel-3.10.0-327.36.3.el7
kernel-tools-libs-3.10.0-327.36.3.el7

noarch
kernel-abi-whitelists-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7

163174 - Oracle Enterprise Linux ELSA-2016-3632 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ELSA-2016-3632

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006428.html
http://oss.oracle.com/pipermail/el-errata/2016-October/006427.html

OEL7
x86_64
kernel-uek-firmware-4.1.12-61.1.16.el7uek
kernel-uek-debug-devel-4.1.12-61.1.16.el7uek

kernel-uek-debug-4.1.12-61.1.16.el7uek
kernel-uek-4.1.12-61.1.16.el7uek
dtrace-modules-4.1.12-61.1.16.el7uek-0.5.3-2.el7
kernel-uek-doc-4.1.12-61.1.16.el7uek
kernel-uek-devel-4.1.12-61.1.16.el7uek

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-61.1.16.el6uek
kernel-uek-doc-4.1.12-61.1.16.el6uek
dtrace-modules-4.1.12-61.1.16.el6uek-0.5.3-2.el6
kernel-uek-firmware-4.1.12-61.1.16.el6uek
kernel-uek-4.1.12-61.1.16.el6uek
kernel-uek-debug-4.1.12-61.1.16.el6uek
kernel-uek-devel-4.1.12-61.1.16.el6uek

163175 - Oracle Enterprise Linux ELSA-2016-2098 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ELSA-2016-2098

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006442.html

OEL7
x86_64
kernel-tools-libs-3.10.0-327.36.3.el7
kernel-tools-3.10.0-327.36.3.el7
kernel-tools-libs-devel-3.10.0-327.36.3.el7
kernel-headers-3.10.0-327.36.3.el7
python-perf-3.10.0-327.36.3.el7
kernel-3.10.0-327.36.3.el7
kernel-debug-devel-3.10.0-327.36.3.el7
perf-3.10.0-327.36.3.el7
kernel-debug-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7
kernel-devel-3.10.0-327.36.3.el7
kernel-abi-whitelists-3.10.0-327.36.3.el7

163176 - Oracle Enterprise Linux ELSA-2016-2094 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776, CVE-2016-2848

Description

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

ELSA-2016-2094

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006423.html

OEL5
i386
bind97-utils-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8

x86_64
bind97-utils-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8

163177 - Oracle Enterprise Linux ELSA-2016-2093 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776, CVE-2016-2848

Description

The scan detected that the host is missing the following update:
ELSA-2016-2093

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006421.html
http://oss.oracle.com/pipermail/el-errata/2016-October/006422.html

OEL5
i386
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

x86_64
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10

bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

OEL6
x86_64
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2

i386
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2

163178 - Oracle Enterprise Linux ELSA-2016-3634 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ELSA-2016-3634

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006431.html
http://oss.oracle.com/pipermail/el-errata/2016-October/006432.html

OEL5
x86_64
kernel-uek-devel-2.6.39-400.286.3.el5uek
kernel-uek-2.6.39-400.286.3.el5uek
kernel-uek-debug-devel-2.6.39-400.286.3.el5uek
kernel-uek-doc-2.6.39-400.286.3.el5uek
kernel-uek-firmware-2.6.39-400.286.3.el5uek
kernel-uek-debug-2.6.39-400.286.3.el5uek

i386
kernel-uek-devel-2.6.39-400.286.3.el5uek
kernel-uek-2.6.39-400.286.3.el5uek
kernel-uek-debug-devel-2.6.39-400.286.3.el5uek
kernel-uek-doc-2.6.39-400.286.3.el5uek
kernel-uek-firmware-2.6.39-400.286.3.el5uek
kernel-uek-debug-2.6.39-400.286.3.el5uek

OEL6
x86_64

kernel-uek-doc-2.6.39-400.286.3.el6uek
kernel-uek-debug-2.6.39-400.286.3.el6uek
kernel-uek-firmware-2.6.39-400.286.3.el6uek
kernel-uek-devel-2.6.39-400.286.3.el6uek
kernel-uek-2.6.39-400.286.3.el6uek
kernel-uek-debug-devel-2.6.39-400.286.3.el6uek

i386
kernel-uek-doc-2.6.39-400.286.3.el6uek
kernel-uek-debug-2.6.39-400.286.3.el6uek
kernel-uek-firmware-2.6.39-400.286.3.el6uek
kernel-uek-devel-2.6.39-400.286.3.el6uek
kernel-uek-2.6.39-400.286.3.el6uek
kernel-uek-debug-devel-2.6.39-400.286.3.el6uek

163179 - Oracle Enterprise Linux ELSA-2016-3633 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-5195

Description
The scan detected that the host is missing the following update:
ELSA-2016-3633

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006430.html
http://oss.oracle.com/pipermail/el-errata/2016-October/006429.html

OEL7
x86_64
kernel-uek-debug-devel-3.8.13-118.13.3.el7uek
kernel-uek-debug-3.8.13-118.13.3.el7uek
kernel-uek-3.8.13-118.13.3.el7uek
dtrace-modules-3.8.13-118.13.3.el7uek-0.4.5-3.el7
kernel-uek-devel-3.8.13-118.13.3.el7uek
kernel-uek-firmware-3.8.13-118.13.3.el7uek
kernel-uek-doc-3.8.13-118.13.3.el7uek

OEL6
x86_64
kernel-uek-devel-3.8.13-118.13.3.el6uek
kernel-uek-doc-3.8.13-118.13.3.el6uek
kernel-uek-debug-devel-3.8.13-118.13.3.el6uek
kernel-uek-debug-3.8.13-118.13.3.el6uek
kernel-uek-firmware-3.8.13-118.13.3.el6uek
dtrace-modules-3.8.13-118.13.3.el6uek-0.4.5-3.el6
kernel-uek-3.8.13-118.13.3.el6uek

163180 - Oracle Enterprise Linux ELSA-2016-2105 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ELSA-2016-2105

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-October/006443.html

OEL6
x86_64
kernel-doc-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-firmware-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

i386
kernel-doc-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-firmware-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6

170737 - Amazon Linux AMI ALAS-2016-760 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000111

Description

The scan detected that the host is missing the following update:
ALAS-2016-760

Observation

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

https://alas.aws.amazon.com/ALAS-2016-760.html

Amazon Linux AMI
x86_64
python27-twisted-web-8.2.0-5.5.amzn1
python26-twisted-web-8.2.0-5.5.amzn1

i686
python27-twisted-web-8.2.0-5.5.amzn1
python26-twisted-web-8.2.0-5.5.amzn1

175026 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1610-6057)

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1610-6057)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=6057

SL7
x86_64
kernel-debug-devel-3.10.0-327.36.3.el7
python-perf-debuginfo-3.10.0-327.36.3.el7
perf-3.10.0-327.36.3.el7
kernel-tools-libs-3.10.0-327.36.3.el7
kernel-devel-3.10.0-327.36.3.el7
kernel-debug-3.10.0-327.36.3.el7
kernel-3.10.0-327.36.3.el7
kernel-debuginfo-common-x86_64-3.10.0-327.36.3.el7
python-perf-3.10.0-327.36.3.el7
kernel-tools-3.10.0-327.36.3.el7
perf-debuginfo-3.10.0-327.36.3.el7
kernel-debug-debuginfo-3.10.0-327.36.3.el7
kernel-debuginfo-3.10.0-327.36.3.el7
kernel-tools-libs-devel-3.10.0-327.36.3.el7
kernel-tools-debuginfo-3.10.0-327.36.3.el7
kernel-headers-3.10.0-327.36.3.el7

noarch
kernel-abi-whitelists-3.10.0-327.36.3.el7
kernel-doc-3.10.0-327.36.3.el7

175027 - Scientific Linux Security ERRATA Important: Important: kernel on SL6.x i386/x86_64 (1610-6382)

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

Risk Level: High

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: Important: kernel on SL6.x i386/x86_64 (1610-6382)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=6382

SL6
i386
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-firmware-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6

noarch
kernel-firmware-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-642.6.2.el6
kernel-debug-2.6.32-642.6.2.el6
kernel-debug-debuginfo-2.6.32-642.6.2.el6
perf-debuginfo-2.6.32-642.6.2.el6
python-perf-2.6.32-642.6.2.el6
kernel-2.6.32-642.6.2.el6
kernel-doc-2.6.32-642.6.2.el6
python-perf-debuginfo-2.6.32-642.6.2.el6
kernel-headers-2.6.32-642.6.2.el6
perf-2.6.32-642.6.2.el6
kernel-debug-devel-2.6.32-642.6.2.el6
kernel-firmware-2.6.32-642.6.2.el6
kernel-abi-whitelists-2.6.32-642.6.2.el6
kernel-debuginfo-2.6.32-642.6.2.el6
kernel-devel-2.6.32-642.6.2.el6
kernel-debuginfo-common-x86_64-2.6.32-642.6.2.el6

182154 - FreeBSD node.js Ares_create_query Single Byte Out Of Buffer Write (28bb6ee5-9b5c-11e6-b799-19bef72f4b7c)

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

Risk Level: High

CVE: CVE-2016-5180

Description

The scan detected that the host is missing the following update:
node.js -- ares_create_query single byte out of buffer write (28bb6ee5-9b5c-11e6-b799-19bef72f4b7c)

Observation

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

http://www.vuxml.org/freebsd/28bb6ee5-9b5c-11e6-b799-19bef72f4b7c.html

Affected packages:
node010 < 0.10.48
node012 < 0.12.17
node4 < 4.6.1

185460 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3112-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5250, CVE-2016-5257, CVE-2016-5270, CVE-2016-5272, CVE-2016-5274, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5280, CVE-2016-5281, CVE-2016-5284

Description

The scan detected that the host is missing the following update:
USN-3112-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003610.html

Ubuntu 12.04

thunderbird_45.4.0+build1-0ubuntu0.12.04.1

Ubuntu 16.04

thunderbird_45.4.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_45.4.0+build1-0ubuntu0.14.04.1

Ubuntu 16.10

thunderbird_45.4.0+build1-0ubuntu0.16.10.1

191305 - Fedora Linux 23 FEDORA-2016-3af8b344f1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

Description

The scan detected that the host is missing the following update:
FEDORA-2016-3af8b344f1

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/2016/10/?count=200&page=2

Fedora Core 23

bind-9.10.4-2.P3.fc23

191309 - Fedora Linux 23 FEDORA-2016-cbef6c8619 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

Description

The scan detected that the host is missing the following update:
FEDORA-2016-cbef6c8619

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/2016/10/?count=200&page=2

Fedora Core 23

bind99-9.9.9-2.P3.fc23

20739 - (JSA10733) Juniper ScreenOS OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-3195

Description

Multiple vulnerabilities are present in some versions of Juniper ScreenOS.

Observation

Juniper ScreenOS is a popular firewall and VPN operating system.

Multiple vulnerabilities are present in some versions of Juniper ScreenOS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

170736 - Amazon Linux AMI ALAS-2016-759 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

The scan detected that the host is missing the following update:
ALAS-2016-759

Observation

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

https://alas.aws.amazon.com/ALAS-2016-759.html

Amazon Linux AMI
i686
java-1.8.0-openjdk-debuginfo-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-src-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-devel-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-demo-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-headless-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-1.8.0.111-1.b15.25.amzn1

noarch
java-1.8.0-openjdk-javadoc-1.8.0.111-1.b15.25.amzn1

x86_64
java-1.8.0-openjdk-devel-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-src-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-demo-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-headless-1.8.0.111-1.b15.25.amzn1
java-1.8.0-openjdk-1.8.0.111-1.b15.25.amzn1

132289 - Oracle VM OVMSA-2016-0145 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2848

Description
The scan detected that the host is missing the following update:
OVMSA-2016-0145

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000563.html
http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000564.html

OVM3.3
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

OVM3.4
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

132290 - Oracle VM OVMSA-2016-0146 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0146

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-October/000565.html

OVM3.2
x86_64
bind-libs-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

141305 - Red Hat Enterprise Linux RHSA-2016-2094 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
RHSA-2016-2094

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2094.html

RHEL5S
i386
bind97-debuginfo-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-utils-9.7.0-21.P2.el5_11.8

x86_64
bind97-debuginfo-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-utils-9.7.0-21.P2.el5_11.8

141309 - Red Hat Enterprise Linux RHSA-2016-2093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
RHSA-2016-2093

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2093.html

RHEL5S
i386
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

x86_64
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

RHEL6D
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

i386
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

RHEL6S
i386
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

x86_64

bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

RHEL6WS
x86_64
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2

i386
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2

RHEL5D
x86_64
bind-sdb-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10

i386
bind-sdb-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10

144961 - SuSE SLES 11 SP4 SUSE-SU-2016:2628-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-7815, CVE-2015-6815, CVE-2016-2391, CVE-2016-2392, CVE-2016-4453, CVE-2016-4454, CVE-2016-5105, CVE-2016-5106, CVE-2016-5107, CVE-2016-5126, CVE-2016-5238, CVE-2016-5337, CVE-2016-5338, CVE-2016-5403, CVE-2016-6490, CVE-2016-7116

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2628-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002352.html

SuSE SLES 11 SP4
i586

kvm-1.4.2-47.1

x86_64
kvm-1.4.2-47.1

160160 - CentOS 5 CESA-2016-2094 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
CESA-2016-2094

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-October/022131.html

CentOS 5
x86_64
bind97-utils-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8

i386
bind97-utils-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8

160161 - CentOS 5, 6 CESA-2016-2093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
CESA-2016-2093

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-October/022127.html
http://lists.centos.org/pipermail/centos-announce/2016-October/022130.html

CentOS 5
x86_64
bind-libbind-devel-9.3.6-25.P1.el5_11.10

bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

i386
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

CentOS 6
x86_64
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2

i686
bind-libs-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-utils-9.8.2-0.47.rc1.el6_8.2

170734 - Amazon Linux AMI ALAS-2016-757 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
ALAS-2016-757

Observation

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

https://alas.aws.amazon.com/ALAS-2016-757.html

Amazon Linux AMI
i686
kernel-debuginfo-common-i686-4.4.23-31.54.amzn1
kernel-debuginfo-4.4.23-31.54.amzn1
kernel-tools-4.4.23-31.54.amzn1
kernel-headers-4.4.23-31.54.amzn1
kernel-devel-4.4.23-31.54.amzn1

kernel-4.4.23-31.54.amzn1
kernel-tools-debuginfo-4.4.23-31.54.amzn1
perf-4.4.23-31.54.amzn1
perf-debuginfo-4.4.23-31.54.amzn1
kernel-tools-devel-4.4.23-31.54.amzn1

noarch
kernel-doc-4.4.23-31.54.amzn1

x86_64
kernel-tools-4.4.23-31.54.amzn1
kernel-tools-devel-4.4.23-31.54.amzn1
kernel-headers-4.4.23-31.54.amzn1
perf-debuginfo-4.4.23-31.54.amzn1
kernel-4.4.23-31.54.amzn1
kernel-tools-debuginfo-4.4.23-31.54.amzn1
perf-4.4.23-31.54.amzn1
kernel-debuginfo-4.4.23-31.54.amzn1
kernel-debuginfo-common-x86_64-4.4.23-31.54.amzn1
kernel-devel-4.4.23-31.54.amzn1

170735 - Amazon Linux AMI ALAS-2016-758 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
ALAS-2016-758

Observation

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

https://alas.aws.amazon.com/ALAS-2016-758.html

Amazon Linux AMI
x86_64
bind-sdb-9.8.2-0.37.rc1.49.amzn1
bind-utils-9.8.2-0.37.rc1.49.amzn1
bind-chroot-9.8.2-0.37.rc1.49.amzn1
bind-debuginfo-9.8.2-0.37.rc1.49.amzn1
bind-devel-9.8.2-0.37.rc1.49.amzn1
bind-libs-9.8.2-0.37.rc1.49.amzn1
bind-9.8.2-0.37.rc1.49.amzn1

i686
bind-sdb-9.8.2-0.37.rc1.49.amzn1
bind-utils-9.8.2-0.37.rc1.49.amzn1
bind-chroot-9.8.2-0.37.rc1.49.amzn1
bind-debuginfo-9.8.2-0.37.rc1.49.amzn1
bind-devel-9.8.2-0.37.rc1.49.amzn1
bind-libs-9.8.2-0.37.rc1.49.amzn1
bind-9.8.2-0.37.rc1.49.amzn1

175024 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1610-5394)

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1610-5394)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=5394

SL5
x86_64
bind97-debuginfo-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-utils-9.7.0-21.P2.el5_11.8

i386
bind97-debuginfo-9.7.0-21.P2.el5_11.8
bind97-chroot-9.7.0-21.P2.el5_11.8
bind97-libs-9.7.0-21.P2.el5_11.8
bind97-9.7.0-21.P2.el5_11.8
bind97-devel-9.7.0-21.P2.el5_11.8
bind97-utils-9.7.0-21.P2.el5_11.8

175025 - Scientific Linux Security ERRATA Important: bind on SL5.x, SL6.x i386/x86_64 (1610-5724)

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL5.x, SL6.x i386/x86_64 (1610-5724)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=5724

SL6
x86_64
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

i386
bind-utils-9.8.2-0.47.rc1.el6_8.2
bind-9.8.2-0.47.rc1.el6_8.2
bind-chroot-9.8.2-0.47.rc1.el6_8.2
bind-sdb-9.8.2-0.47.rc1.el6_8.2
bind-debuginfo-9.8.2-0.47.rc1.el6_8.2
bind-devel-9.8.2-0.47.rc1.el6_8.2
bind-libs-9.8.2-0.47.rc1.el6_8.2

SL5
x86_64
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

i386
bind-debuginfo-9.3.6-25.P1.el5_11.10
bind-libbind-devel-9.3.6-25.P1.el5_11.10
bind-libs-9.3.6-25.P1.el5_11.10
bind-devel-9.3.6-25.P1.el5_11.10
bind-sdb-9.3.6-25.P1.el5_11.10
bind-chroot-9.3.6-25.P1.el5_11.10
caching-nameserver-9.3.6-25.P1.el5_11.10
bind-9.3.6-25.P1.el5_11.10
bind-utils-9.3.6-25.P1.el5_11.10

182150 - FreeBSD Axis2 Security Vulnerabilities On Dependency Apache HttpClient (ac18046c-9b08-11e6-8011-005056925db4)

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

Risk Level: Medium

CVE: CVE-2012-6153, CVE-2014-3577

Description

The scan detected that the host is missing the following update:
Axis2 -- Security vulnerabilities on dependency Apache HttpClient (ac18046c-9b08-11e6-8011-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/ac18046c-9b08-11e6-8011-005056925db4.html

Affected packages:
axis2 < 1.7.4

185457 - Ubuntu Linux 12.04 USN-3108-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2848

Description

The scan detected that the host is missing the following update:
USN-3108-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003603.html

Ubuntu 12.04

bind9_9.8.1.dfsg.P1-4ubuntu0.18

144966 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2589-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2391, CVE-2016-2392, CVE-2016-4453, CVE-2016-4454, CVE-2016-5105, CVE-2016-5106, CVE-2016-5107, CVE-2016-5126, CVE-2016-5238, CVE-2016-5337, CVE-2016-5338, CVE-2016-5403, CVE-2016-6490, CVE-2016-6833, CVE-2016-6836, CVE-2016-6888, CVE-2016-7116, CVE-2016-7155, CVE-2016-7156

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2589-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002344.html

SuSE SLES 12 SP1
noarch
qemu-sgabios-8-21.1
qemu-ipxe-1.0.0-21.1
qemu-vgabios-1.8.1-21.1
qemu-seabios-1.8.1-21.1

x86_64
qemu-block-rbd-2.3.1-21.1
qemu-block-curl-2.3.1-21.1
qemu-2.3.1-21.1
qemu-lang-2.3.1-21.1
qemu-block-rbd-debuginfo-2.3.1-21.1
qemu-debugsource-2.3.1-21.1
qemu-tools-debuginfo-2.3.1-21.1
qemu-guest-agent-2.3.1-21.1
qemu-guest-agent-debuginfo-2.3.1-21.1
qemu-kvm-2.3.1-21.1
qemu-block-curl-debuginfo-2.3.1-21.1
qemu-tools-2.3.1-21.1
qemu-x86-2.3.1-21.1

SuSE SLED 12 SP1
x86_64

qemu-x86-2.3.1-21.1
qemu-kvm-2.3.1-21.1
qemu-2.3.1-21.1
qemu-debugsource-2.3.1-21.1
qemu-block-curl-2.3.1-21.1
qemu-block-curl-debuginfo-2.3.1-21.1
qemu-tools-debuginfo-2.3.1-21.1
qemu-tools-2.3.1-21.1

noarch
qemu-sgabios-8-21.1
qemu-ipxe-1.0.0-21.1
qemu-vgabios-1.8.1-21.1
qemu-seabios-1.8.1-21.1

182153 - FreeBSD node.js Multiple Vulnerabilities (27180c99-9b5c-11e6-b799-19bef72f4b7c)

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

Risk Level: Medium

CVE: CVE-2016-5172

Description

The scan detected that the host is missing the following update:
node.js -- multiple vulnerabilities (27180c99-9b5c-11e6-b799-19bef72f4b7c)

Observation

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

http://www.vuxml.org/freebsd/27180c99-9b5c-11e6-b799-19bef72f4b7c.html

Affected packages:
6.0.0 <= node < 6.9.0

130613 - Debian Linux 8.0 DSA-3697-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7966

Description

The scan detected that the host is missing the following update:
DSA-3697-1

Observation

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

http://www.debian.org/security/2016/dsa-3697

Debian 8.0
all
libkpimidentities4_4:4.14.2-2+deb8u2
kdepimlibs5-dev_4:4.14.2-2+deb8u2
libkblog4_4:4.14.2-2+deb8u2
libkldap4_4:4.14.2-2+deb8u2

libakonadi-contact4_4:4.14.2-2+deb8u2
libkmime4_4:4.14.2-2+deb8u2
libakonadi-notes4_4:4.14.2-2+deb8u2
libkpimtextedit4_4:4.14.2-2+deb8u2
libkontactinterface4a_4:4.14.2-2+deb8u2
libakonadi-kcal4_4:4.14.2-2+deb8u2
libakonadi-kabc4_4:4.14.2-2+deb8u2
libkxmlrpcclient4_4:4.14.2-2+deb8u2
kdepimlibs-kio-plugins_4:4.14.2-2+deb8u2
libakonadi-xml4_4:4.14.2-2+deb8u2
libkholidays4_4:4.14.2-2+deb8u2
libmailtransport4_4:4.14.2-2+deb8u2
libmicroblog4_4:4.14.2-2+deb8u2
libakonadi-kmime4_4:4.14.2-2+deb8u2
libakonadi-kde4_4:4.14.2-2+deb8u2
kdepimlibs-dbg_4:4.14.2-2+deb8u2
libkabc4_4:4.14.2-2+deb8u2
libqgpgme1_4:4.14.2-2+deb8u2
libakonadi-calendar4_4:4.14.2-2+deb8u2
libktnef4_4:4.14.2-2+deb8u2
libkcalutils4_4:4.14.2-2+deb8u2
libkcalcore4_4:4.14.2-2+deb8u2
libkcal4_4:4.14.2-2+deb8u2
libgpgme++2_4:4.14.2-2+deb8u2
libkalarmcal2_4:4.14.2-2+deb8u2
libkpimutils4_4:4.14.2-2+deb8u2
libsyndication4_4:4.14.2-2+deb8u2
libkimap4_4:4.14.2-2+deb8u2
libkresources4_4:4.14.2-2+deb8u2
libkmbox4_4:4.14.2-2+deb8u2
libakonadi-socialutils4_4:4.14.2-2+deb8u2

130614 - Debian Linux 8.0 DSA-3698-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-MAP-NOMATCH

Description
The scan detected that the host is missing the following update:
DSA-3698-1

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

http://www.debian.org/security/2016/dsa-3698

Debian 8.0
all
php5_5.6.27+dfsg-0+deb8u1

130616 - Debian Linux 8.0 DSA-3701-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-1247

Description

The scan detected that the host is missing the following update:
DSA-3701-1

Observation

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

http://www.debian.org/security/2016/dsa-3701

Debian 8.0
all
nginx_1.6.2-5+deb8u3

144941 - SuSE Linux 13.2 openSUSE-SU-2016:2643-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8605

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2643-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00096.html

SuSE Linux 13.2
x86_64
guile1-debugsource-1.8.8-16.3.1
guile1-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-13-14-v-3-3-1.8.8-16.3.1
libguile-srfi-srfi-1-v-3-3-1.8.8-16.3.1
libguile1-devel-1.8.8-16.3.1
libguilereadline-v-17-17-1.8.8-16.3.1
libguile-srfi-srfi-60-v-2-2-1.8.8-16.3.1
libguile-srfi-srfi-1-v-3-3-debuginfo-1.8.8-16.3.1
libguile17-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-4-v-3-3-debuginfo-1.8.8-16.3.1
libguile17-1.8.8-16.3.1
guile1-1.8.8-16.3.1
libguile-srfi-srfi-60-v-2-2-debuginfo-1.8.8-16.3.1
libguilereadline-v-17-17-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-4-v-3-3-1.8.8-16.3.1
libguile-srfi-srfi-13-14-v-3-3-debuginfo-1.8.8-16.3.1

i586
guile1-debugsource-1.8.8-16.3.1
guile1-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-13-14-v-3-3-1.8.8-16.3.1
libguile-srfi-srfi-1-v-3-3-1.8.8-16.3.1
libguile1-devel-1.8.8-16.3.1
libguilereadline-v-17-17-1.8.8-16.3.1

libguile-srfi-srfi-60-v-2-2-1.8.8-16.3.1
libguile-srfi-srfi-1-v-3-3-debuginfo-1.8.8-16.3.1
libguile17-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-4-v-3-3-debuginfo-1.8.8-16.3.1
libguile17-1.8.8-16.3.1
guile1-1.8.8-16.3.1
libguile-srfi-srfi-60-v-2-2-debuginfo-1.8.8-16.3.1
libguilereadline-v-17-17-debuginfo-1.8.8-16.3.1
libguile-srfi-srfi-4-v-3-3-1.8.8-16.3.1
libguile-srfi-srfi-13-14-v-3-3-debuginfo-1.8.8-16.3.1

144947 - SuSE Linux 13.2 openSUSE-SU-2016:2645-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8605, CVE-2016-8606

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2645-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-10/msg00098.html

SuSE Linux 13.2
x86_64
guile-devel-2.0.11-3.3.1
guile-debuginfo-2.0.11-3.3.1
guile-debugsource-2.0.11-3.3.1
guile-modules-2_0-2.0.11-3.3.1
guile-2.0.11-3.3.1
libguilereadline-v-18-18-2.0.11-3.3.1
libguile-2_0-22-debuginfo-2.0.11-3.3.1
libguile-2_0-22-2.0.11-3.3.1
libguilereadline-v-18-18-debuginfo-2.0.11-3.3.1

i586
guile-devel-2.0.11-3.3.1
guile-debuginfo-2.0.11-3.3.1
guile-debugsource-2.0.11-3.3.1
guile-modules-2_0-2.0.11-3.3.1
guile-2.0.11-3.3.1
libguilereadline-v-18-18-2.0.11-3.3.1
libguile-2_0-22-debuginfo-2.0.11-3.3.1
libguile-2_0-22-2.0.11-3.3.1
libguilereadline-v-18-18-debuginfo-2.0.11-3.3.1

144949 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2579-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-0249

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2579-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-October/002342.html

SuSE SLES 12 SP1
x86_64
sssd-tools-debuginfo-1.11.5.1-28.1
sssd-32bit-1.11.5.1-28.1
sssd-proxy-1.11.5.1-28.1
python-sssd-config-1.11.5.1-28.1
sssd-ad-1.11.5.1-28.1
sssd-debuginfo-32bit-1.11.5.1-28.1
sssd-ldap-debuginfo-1.11.5.1-28.1
libsss_sudo-debuginfo-1.11.5.1-28.1
sssd-krb5-debuginfo-1.11.5.1-28.1
sssd-proxy-debuginfo-1.11.5.1-28.1
libsss_sudo-1.11.5.1-28.1
sssd-tools-1.11.5.1-28.1
sssd-debuginfo-1.11.5.1-28.1
libipa_hbac0-1.11.5.1-28.1
libipa_hbac0-debuginfo-1.11.5.1-28.1
sssd-krb5-common-1.11.5.1-28.1
sssd-1.11.5.1-28.1
sssd-krb5-common-debuginfo-1.11.5.1-28.1
python-sssd-config-debuginfo-1.11.5.1-28.1
libsss_idmap0-debuginfo-1.11.5.1-28.1
sssd-krb5-1.11.5.1-28.1
libsss_idmap0-1.11.5.1-28.1
sssd-ldap-1.11.5.1-28.1
sssd-ad-debuginfo-1.11.5.1-28.1
sssd-ipa-debuginfo-1.11.5.1-28.1
sssd-ipa-1.11.5.1-28.1
sssd-debugsource-1.11.5.1-28.1

SuSE SLED 12 SP1
x86_64
sssd-tools-debuginfo-1.11.5.1-28.1
sssd-32bit-1.11.5.1-28.1
sssd-proxy-1.11.5.1-28.1
python-sssd-config-1.11.5.1-28.1
sssd-ad-1.11.5.1-28.1
sssd-debuginfo-32bit-1.11.5.1-28.1
sssd-ldap-debuginfo-1.11.5.1-28.1
libsss_sudo-debuginfo-1.11.5.1-28.1
sssd-krb5-debuginfo-1.11.5.1-28.1
sssd-proxy-debuginfo-1.11.5.1-28.1
libsss_sudo-1.11.5.1-28.1
sssd-tools-1.11.5.1-28.1
sssd-debuginfo-1.11.5.1-28.1
libipa_hbac0-1.11.5.1-28.1
libipa_hbac0-debuginfo-1.11.5.1-28.1
sssd-krb5-common-1.11.5.1-28.1
sssd-1.11.5.1-28.1
sssd-krb5-common-debuginfo-1.11.5.1-28.1
python-sssd-config-debuginfo-1.11.5.1-28.1

libsss_idmap0-debuginfo-1.11.5.1-28.1
sssd-krb5-1.11.5.1-28.1
libsss_idmap0-1.11.5.1-28.1
sssd-ldap-1.11.5.1-28.1
sssd-ad-debuginfo-1.11.5.1-28.1
sssd-ipa-debuginfo-1.11.5.1-28.1
sssd-ipa-1.11.5.1-28.1
sssd-debugsource-1.11.5.1-28.1

182149 - FreeBSD urllib3 Certificate Verification Failure (c5c6e293-9cc7-11e6-823f-b8aeed92ecc4)

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

Risk Level: Low

CVE: CVE-2016-9015

Description

The scan detected that the host is missing the following update:
urllib3 -- certificate verification failure (c5c6e293-9cc7-11e6-823f-b8aeed92ecc4)

Observation

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

http://www.vuxml.org/freebsd/c5c6e293-9cc7-11e6-823f-b8aeed92ecc4.html

Affected packages:
py-urllib3 < 1.18

182151 - FreeBSD mozilla Multiple Vulnerabilities (aaa9f3db-13b5-4a0e-9ed7-e5ab287098fa)

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

Risk Level: Low

CVE: CVE-2016-5287, CVE-2016-5288

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (aaa9f3db-13b5-4a0e-9ed7-e5ab287098fa)

Observation

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

http://www.vuxml.org/freebsd/aaa9f3db-13b5-4a0e-9ed7-e5ab287098fa.html

Affected packages:
firefox < 49.0.2,1

182152 - FreeBSD flash Remote Code Execution (de6d01d5-9c44-11e6-ba67-0011d823eebd)

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

Risk Level: Low

CVE: CVE-2016-7855

Description

The scan detected that the host is missing the following update:
flash -- remote code execution (de6d01d5-9c44-11e6-ba67-0011d823eebd)

Observation

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

http://www.vuxml.org/freebsd/de6d01d5-9c44-11e6-ba67-0011d823eebd.html

Affected packages:
linux-f10-flashplugin < 11.2r202.643
linux-c6-flashplugin < 11.2r202.643
linux-c7-flashplugin < 11.2r202.643

182155 - FreeBSD FreeBSD Bhyve - Privilege Escalation Vulnerability (a479a725-9adb-11e6-a298-14dae9d210b8)

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:
FreeBSD -- bhyve - privilege escalation vulnerability (a479a725-9adb-11e6-a298-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/a479a725-9adb-11e6-a298-14dae9d210b8.html

Affected packages:
11.0 <= FreeBSD-kernel < 11.0_2

185456 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3114-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1247

Description

The scan detected that the host is missing the following update:
USN-3114-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003607.html

Ubuntu 16.04

nginx-common_1.10.0-0ubuntu0.16.04.3
nginx-light_1.10.0-0ubuntu0.16.04.3
nginx-full_1.10.0-0ubuntu0.16.04.3
nginx-core_1.10.0-0ubuntu0.16.04.3

nginx-extras_1.10.0-0ubuntu0.16.04.3

Ubuntu 14.04

nginx-common_1.4.6-1ubuntu3.6
nginx-extras_1.4.6-1ubuntu3.6
nginx-core_1.4.6-1ubuntu3.6
nginx-full_1.4.6-1ubuntu3.6
nginx-light_1.4.6-1ubuntu3.6

Ubuntu 16.10

nginx-common_1.10.1-0ubuntu1.1
nginx-core_1.10.1-0ubuntu1.1
nginx-extras_1.10.1-0ubuntu1.1
nginx-full_1.10.1-0ubuntu1.1
nginx-light_1.10.1-0ubuntu1.1

185458 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3111-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5287, CVE-2016-5288

Description

The scan detected that the host is missing the following update:
USN-3111-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003609.html

Ubuntu 12.04

firefox_49.0.2+build2-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_49.0.2+build2-0ubuntu0.16.04.2

Ubuntu 14.04

firefox_49.0.2+build2-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_49.0.2+build2-0ubuntu0.16.10.2

185459 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3114-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3114-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003608.html

Ubuntu 16.04

nginx-core_1.10.0-0ubuntu0.16.04.4
nginx-light_1.10.0-0ubuntu0.16.04.4
nginx-full_1.10.0-0ubuntu0.16.04.4
nginx-extras_1.10.0-0ubuntu0.16.04.4
nginx-common_1.10.0-0ubuntu0.16.04.4

Ubuntu 14.04

nginx-light_1.4.6-1ubuntu3.7
nginx-core_1.4.6-1ubuntu3.7
nginx-extras_1.4.6-1ubuntu3.7
nginx-full_1.4.6-1ubuntu3.7
nginx-common_1.4.6-1ubuntu3.7

Ubuntu 16.10

nginx-light_1.10.1-0ubuntu1.2
nginx-full_1.10.1-0ubuntu1.2
nginx-common_1.10.1-0ubuntu1.2
nginx-extras_1.10.1-0ubuntu1.2
nginx-core_1.10.1-0ubuntu1.2

185461 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3110-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1245

Description

The scan detected that the host is missing the following update:
USN-3110-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003606.html

Ubuntu 12.04

quagga_0.99.20.1-0ubuntu0.12.04.6

Ubuntu 16.04

quagga_0.99.24.1-2ubuntu1.2

Ubuntu 14.04

quagga_0.99.22.4-3ubuntu1.3

Ubuntu 16.10

quagga_1.0.20160315-2ubuntu0.1

185462 - Ubuntu Linux 16.10 USN-3107-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
USN-3107-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003604.html

Ubuntu 16.10

linux-image-4.8.0-1017-raspi2_4.8.0-1017.20

185463 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3109-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5584, CVE-2016-7440

Description

The scan detected that the host is missing the following update:
USN-3109-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003605.html

Ubuntu 12.04

mysql-server-5.5_5.5.53-0ubuntu0.12.04.1

Ubuntu 16.04

mysql-server-5.7_5.7.16-0ubuntu0.16.04.1

Ubuntu 14.04

mysql-server-5.5_5.5.53-0ubuntu0.14.04.1

Ubuntu 16.10

mysql-server-5.7_5.7.16-0ubuntu0.16.10.1

191296 - Fedora Linux 23 FEDORA-2016-a47bf58beb Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-8605, CVE-2016-8606

Description
The scan detected that the host is missing the following update:
FEDORA-2016-a47bf58beb

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/2016/10/?count=200&page=4

Fedora Core 23

guile-2.0.13-1.fc23

191297 - Fedora Linux 23 FEDORA-2016-0729e59542 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-2016-0729e59542

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/2016/10/?count=200&page=3

Fedora Core 23

php-5.6.27-1.fc23

191298 - Fedora Linux 23 FEDORA-2016-c3558808cd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5195

Description
The scan detected that the host is missing the following update:
FEDORA-2016-c3558808cd

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/2016/10/?count=200&page=3

Fedora Core 23

kernel-4.7.9-100.fc23

191299 - Fedora Linux 25 FEDORA-2016-81f9c6f0ae Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693

Description

The scan detected that the host is missing the following update:
FEDORA-2016-81f9c6f0ae

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/2016/10/?count=200&page=1

Fedora Core 25

jasper-1.900.13-1.fc25

191300 - Fedora Linux 24 FEDORA-2016-db4b75b352 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
FEDORA-2016-db4b75b352

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/2016/10/?count=200&page=3

Fedora Core 24

kernel-4.7.9-200.fc24

191301 - Fedora Linux 23 FEDORA-2016-f8fd3891f8 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-2016-f8fd3891f8

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/2016/10/?count=200&page=2

Fedora Core 23

perl-Image-Info-1.38-6.fc23

191302 - Fedora Linux 23 FEDORA-2016-616a35205b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8568, CVE-2016-8569

Description

The scan detected that the host is missing the following update:
FEDORA-2016-616a35205b

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/2016/10/?count=200&page=4

Fedora Core 23

libgit2-0.23.4-2.fc23

191303 - Fedora Linux 25 FEDORA-2016-d2a05a0644 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7969, CVE-2016-7970, CVE-2016-7971, CVE-2016-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2016-d2a05a0644

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/2016/10/?count=200&page=1

Fedora Core 25

libass-0.13.4-1.fc25

191304 - Fedora Linux 23 FEDORA-2016-0312cf1dcd 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-2016-0312cf1dcd

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/2016/10/?count=200&page=3

Fedora Core 23

php-pecl-zip-1.13.5-1.fc23

191306 - Fedora Linux 24 FEDORA-2016-b9cb75981a 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-2016-b9cb75981a

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/2016/10/?count=200&page=3

Fedora Core 24

php-pecl-zip-1.13.5-1.fc24

191307 - Fedora Linux 24 FEDORA-2016-be779371b4 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-2016-be779371b4

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/2016/10/?count=200&page=2

Fedora Core 24

perl-Image-Info-1.38-6.fc24

191308 - Fedora Linux 25 FEDORA-2016-c8a0c7eece Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5195

Description

The scan detected that the host is missing the following update:
FEDORA-2016-c8a0c7eece

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/2016/10/?count=200&page=3

Fedora Core 25

kernel-4.8.3-300.fc25

191310 - Fedora Linux 24 FEDORA-2016-7a30285647 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-2016-7a30285647

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/2016/10/?count=200&page=3

Fedora Core 24

php-5.6.27-1.fc24

191311 - Fedora Linux 24 FEDORA-2016-282507c3e9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7969, CVE-2016-7970, CVE-2016-7971, CVE-2016-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2016-282507c3e9

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/2016/10/?count=200&page=2

Fedora Core 24

libass-0.13.4-1.fc24

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.

141302 - Red Hat Enterprise Linux RHSA-2016-2088 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

141303 - Red Hat Enterprise Linux RHSA-2016-2090 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

141304 - Red Hat Enterprise Linux RHSA-2016-2089 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

160157 - CentOS 6, 7 CESA-2016-2079 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

163173 - Oracle Enterprise Linux ELSA-2016-2079 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

175023 - Scientific Linux Security ERRATA Critical: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1610-4967)

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

Risk Level: Medium

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

Risk is updated

182062 - FreeBSD FreeBSD Incorrect Argument Validation In Sysarch (2) (7b6a11b5-600a-11e6-a6c3-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2016-1885

Update Details

FASLScript is updated

33307 - Oracle Solaris 151934-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript 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.