2016-MAY-12
FSL version 7.5.822

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

19999 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.8

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

20000 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.8

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

20001 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.1

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

Risk Level: High

CVE: CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

20002 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

20059 - IBM AIX Java Multiple Vulnerabilities (April 2016)

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

Risk Level: High

CVE: CVE-2013-3009, CVE-2013-5456, CVE-2016-0264, CVE-2016-0363, CVE-2016-0376, CVE-2016-0686, CVE-2016-0687, CVE-2016-3422, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in Java. Successful exploitation could allow an attacker to impact confidentiality, integrity and availability.

20073 - EMC Unisphere for VMAX Virtual Appliance Arbitrary File Upload Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0889

Description

An arbitrary file upload vulnerability is present in some versions of EMC Unisphere for VMAX Virtual Appliance.

Observation

EMC Unisphere is a web-based product which provides an interface for remote storage management.

An arbitrary file upload vulnerability is present in some versions of EMC Unisphere for VMAX Virtual Appliance. The flaw lies in an HTTP servlet in vApp Manager. Successful exploitation could allow an attacker to compromise integrity, confidentiality or availability of the affected system. Exploitation of this vulnerability doesn't require authentication.

141179 - Red Hat Enterprise Linux RHSA-2016-0722 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
RHSA-2016-0722

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0722.html

RHEL7D
x86_64
openssl-static-1.0.1e-51.el7_2.5
openssl-debuginfo-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-devel-1.0.1e-51.el7_2.5

RHEL7S
ppc64
openssl-static-1.0.1e-51.el7_2.5
openssl-debuginfo-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-devel-1.0.1e-51.el7_2.5

RHEL7WS
x86_64
openssl-static-1.0.1e-51.el7_2.5
openssl-debuginfo-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-devel-1.0.1e-51.el7_2.5

141180 - Red Hat Enterprise Linux RHSA-2016-0726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
RHSA-2016-0726

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0726.html

RHEL7S
ppc64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-debuginfo-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2

RHEL6S
i386
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

x86_64
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

RHEL6WS
x86_64
ImageMagick-c++-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7

i386
ImageMagick-c++-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7

RHEL7D
x86_64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-debuginfo-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2

RHEL6D
x86_64
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

i386
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

RHEL7WS
x86_64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-debuginfo-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2

141184 - Red Hat Enterprise Linux RHSA-2016-0723 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
RHSA-2016-0723

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0723.html

RHEL5S
x86_64
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

i386
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

RHEL7S
x86_64
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2

java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2

RHEL6S
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

i386
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

RHEL6WS
x86_64
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7

i386
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7

RHEL5D
x86_64
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

i386
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

RHEL7D
x86_64
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2

RHEL6D

x86_64
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

i386
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

RHEL7WS
x86_64
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2

141185 - Red Hat Enterprise Linux RHSA-2016-0996 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
RHSA-2016-0996

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0996.html

RHEL6D
x86_64
openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

i386
openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

RHEL6S
i386

openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

x86_64
openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

RHEL6WS
x86_64
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1

i386
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1

144581 - SuSE Linux 13.1 openSUSE-SU-2016:1251-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2804, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2809, CVE-2016-2810, CVE-2016-2811, CVE-2016-2812, CVE-2016-2813, CVE-2016-2814, CVE-2016-2816, CVE-2016-2817, CVE-2016-2820

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1251-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00038.html

SuSE Linux 13.1
x86_64
libsoftokn3-debuginfo-3.22.3-77.1
mozilla-nss-sysinit-debuginfo-3.22.3-77.1
mozilla-nss-certs-3.22.3-77.1
libfreebl3-debuginfo-3.22.3-77.1
mozilla-nss-sysinit-32bit-3.22.3-77.1
mozilla-nss-sysinit-debuginfo-32bit-3.22.3-77.1
MozillaFirefox-translations-other-46.0-113.2
MozillaFirefox-translations-common-46.0-113.2
mozilla-nss-debugsource-3.22.3-77.1
mozilla-nss-sysinit-3.22.3-77.1
mozilla-nss-certs-debuginfo-32bit-3.22.3-77.1
libsoftokn3-32bit-3.22.3-77.1
mozilla-nss-devel-3.22.3-77.1
libsoftokn3-3.22.3-77.1
MozillaFirefox-branding-upstream-46.0-113.2

mozilla-nss-certs-debuginfo-3.22.3-77.1
MozillaFirefox-buildsymbols-46.0-113.2
MozillaFirefox-debugsource-46.0-113.2
MozillaFirefox-46.0-113.2
libfreebl3-3.22.3-77.1
libfreebl3-32bit-3.22.3-77.1
mozilla-nss-32bit-3.22.3-77.1
mozilla-nss-debuginfo-3.22.3-77.1
mozilla-nss-3.22.3-77.1
mozilla-nss-debuginfo-32bit-3.22.3-77.1
libfreebl3-debuginfo-32bit-3.22.3-77.1
libsoftokn3-debuginfo-32bit-3.22.3-77.1
mozilla-nss-certs-32bit-3.22.3-77.1
MozillaFirefox-debuginfo-46.0-113.2
MozillaFirefox-devel-46.0-113.2
mozilla-nss-tools-debuginfo-3.22.3-77.1
mozilla-nss-tools-3.22.3-77.1

i586
libsoftokn3-3.22.3-77.1
mozilla-nss-tools-debuginfo-3.22.3-77.1
mozilla-nss-certs-debuginfo-3.22.3-77.1
mozilla-nss-devel-3.22.3-77.1
libfreebl3-3.22.3-77.1
MozillaFirefox-devel-46.0-113.2
mozilla-nss-debuginfo-3.22.3-77.1
MozillaFirefox-branding-upstream-46.0-113.2
mozilla-nss-tools-3.22.3-77.1
mozilla-nss-sysinit-3.22.3-77.1
MozillaFirefox-buildsymbols-46.0-113.2
MozillaFirefox-46.0-113.2
MozillaFirefox-translations-other-46.0-113.2
MozillaFirefox-translations-common-46.0-113.2
mozilla-nss-3.22.3-77.1
MozillaFirefox-debuginfo-46.0-113.2
libfreebl3-debuginfo-3.22.3-77.1
mozilla-nss-sysinit-debuginfo-3.22.3-77.1
mozilla-nss-certs-3.22.3-77.1
mozilla-nss-debugsource-3.22.3-77.1
libsoftokn3-debuginfo-3.22.3-77.1
MozillaFirefox-debugsource-46.0-113.2

144582 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1248-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1248-1

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-May/002044.html

SuSE SLES 12 SP1
x86_64
java-1_8_0-openjdk-debuginfo-1.8.0.91-11.1
java-1_8_0-openjdk-demo-1.8.0.91-11.1
java-1_8_0-openjdk-debugsource-1.8.0.91-11.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.91-11.1
java-1_8_0-openjdk-devel-1.8.0.91-11.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.91-11.1
java-1_8_0-openjdk-headless-1.8.0.91-11.1
java-1_8_0-openjdk-1.8.0.91-11.1

SuSE SLED 12 SP1
x86_64
java-1_8_0-openjdk-debugsource-1.8.0.91-11.1
java-1_8_0-openjdk-headless-1.8.0.91-11.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.91-11.1
java-1_8_0-openjdk-1.8.0.91-11.1
java-1_8_0-openjdk-debuginfo-1.8.0.91-11.1

144583 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1260-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1260-1

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-May/002049.html

SuSE SLES 12
x86_64
libMagickWand-6_Q16-1-6.8.8.1-19.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-19.1
ImageMagick-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-6.8.8.1-19.1
ImageMagick-debugsource-6.8.8.1-19.1

SuSE SLES 12 SP1
x86_64
libMagickWand-6_Q16-1-6.8.8.1-19.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-19.1
ImageMagick-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-6.8.8.1-19.1
ImageMagick-debugsource-6.8.8.1-19.1

SuSE SLED 12
x86_64
libMagickWand-6_Q16-1-6.8.8.1-19.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-19.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-19.1

libMagickCore-6_Q16-1-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-19.1
ImageMagick-debugsource-6.8.8.1-19.1
ImageMagick-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-19.1
ImageMagick-6.8.8.1-19.1
libMagickCore-6_Q16-1-6.8.8.1-19.1
libMagick++-6_Q16-3-6.8.8.1-19.1

SuSE SLED 12 SP1
x86_64
libMagickWand-6_Q16-1-6.8.8.1-19.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-19.1
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-19.1
ImageMagick-debugsource-6.8.8.1-19.1
ImageMagick-debuginfo-6.8.8.1-19.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-19.1
ImageMagick-6.8.8.1-19.1
libMagickCore-6_Q16-1-6.8.8.1-19.1
libMagick++-6_Q16-3-6.8.8.1-19.1

144584 - SuSE Linux 13.2 openSUSE-SU-2016:1242-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-2105, CVE-2016-2106, CVE-2016-2108, CVE-2016-2109

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1242-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00036.html

SuSE Linux 13.2
x86_64
libopenssl0_9_8-32bit-0.9.8zh-9.6.1
libopenssl0_9_8-debugsource-0.9.8zh-9.6.1
libopenssl0_9_8-0.9.8zh-9.6.1
libopenssl0_9_8-debuginfo-32bit-0.9.8zh-9.6.1
libopenssl0_9_8-debuginfo-0.9.8zh-9.6.1

i586
libopenssl0_9_8-debugsource-0.9.8zh-9.6.1
libopenssl0_9_8-0.9.8zh-9.6.1
libopenssl0_9_8-debuginfo-0.9.8zh-9.6.1

144585 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1258-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2807, CVE-2016-2808, CVE-2016-2814

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1258-1

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-May/002047.html

SuSE SLED 12 SP1
x86_64
MozillaFirefox-debuginfo-38.8.0esr-66.2
MozillaFirefox-debugsource-38.8.0esr-66.2
MozillaFirefox-translations-38.8.0esr-66.2
MozillaFirefox-38.8.0esr-66.2

SuSE SLED 12
x86_64
MozillaFirefox-debuginfo-38.8.0esr-66.2
MozillaFirefox-debugsource-38.8.0esr-66.2
MozillaFirefox-translations-38.8.0esr-66.2
MozillaFirefox-38.8.0esr-66.2

SuSE SLES 12 SP1
x86_64
MozillaFirefox-debuginfo-38.8.0esr-66.2
MozillaFirefox-debugsource-38.8.0esr-66.2
MozillaFirefox-translations-38.8.0esr-66.2
MozillaFirefox-38.8.0esr-66.2

SuSE SLES 12
x86_64
MozillaFirefox-debuginfo-38.8.0esr-66.2
MozillaFirefox-debugsource-38.8.0esr-66.2
MozillaFirefox-translations-38.8.0esr-66.2
MozillaFirefox-38.8.0esr-66.2

144589 - SuSE SLED 12, 12 SP1 SUSE-SU-2016:1267-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-2105, CVE-2016-2106, CVE-2016-2108, CVE-2016-2109

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1267-1

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-May/002050.html

SuSE SLED 12
x86_64

libopenssl0_9_8-32bit-0.9.8j-97.1
compat-openssl098-debugsource-0.9.8j-97.1
libopenssl0_9_8-debuginfo-0.9.8j-97.1
libopenssl0_9_8-0.9.8j-97.1
libopenssl0_9_8-debuginfo-32bit-0.9.8j-97.1

SuSE SLED 12 SP1
x86_64
libopenssl0_9_8-32bit-0.9.8j-97.1
compat-openssl098-debugsource-0.9.8j-97.1
libopenssl0_9_8-debuginfo-0.9.8j-97.1
libopenssl0_9_8-0.9.8j-97.1
libopenssl0_9_8-debuginfo-32bit-0.9.8j-97.1

144590 - SuSE Linux 13.2 openSUSE-SU-2016:1261-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1261-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00041.html

SuSE Linux 13.2
i586
libMagickWand-6_Q16-2-6.8.9.8-18.1
ImageMagick-6.8.9.8-18.1
ImageMagick-debugsource-6.8.9.8-18.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-18.1
ImageMagick-debuginfo-6.8.9.8-18.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-18.1
perl-PerlMagick-6.8.9.8-18.1
ImageMagick-extra-6.8.9.8-18.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-18.1
perl-PerlMagick-debuginfo-6.8.9.8-18.1
ImageMagick-devel-6.8.9.8-18.1
libMagick++-devel-6.8.9.8-18.1
ImageMagick-extra-debuginfo-6.8.9.8-18.1
libMagick++-6_Q16-5-6.8.9.8-18.1
libMagickCore-6_Q16-2-6.8.9.8-18.1

noarch
ImageMagick-doc-6.8.9.8-18.1

x86_64
libMagickWand-6_Q16-2-debuginfo-32bit-6.8.9.8-18.1
libMagickWand-6_Q16-2-6.8.9.8-18.1
ImageMagick-6.8.9.8-18.1
ImageMagick-debugsource-6.8.9.8-18.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-18.1
ImageMagick-debuginfo-6.8.9.8-18.1

libMagick++-6_Q16-5-debuginfo-6.8.9.8-18.1
perl-PerlMagick-6.8.9.8-18.1
ImageMagick-extra-6.8.9.8-18.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-18.1
libMagickCore-6_Q16-2-debuginfo-32bit-6.8.9.8-18.1
libMagick++-devel-32bit-6.8.9.8-18.1
libMagickCore-6_Q16-2-32bit-6.8.9.8-18.1
libMagick++-6_Q16-5-debuginfo-32bit-6.8.9.8-18.1
ImageMagick-devel-32bit-6.8.9.8-18.1
libMagick++-6_Q16-5-32bit-6.8.9.8-18.1
libMagickWand-6_Q16-2-32bit-6.8.9.8-18.1
perl-PerlMagick-debuginfo-6.8.9.8-18.1
ImageMagick-devel-6.8.9.8-18.1
libMagick++-devel-6.8.9.8-18.1
ImageMagick-extra-debuginfo-6.8.9.8-18.1
libMagick++-6_Q16-5-6.8.9.8-18.1
libMagickCore-6_Q16-2-6.8.9.8-18.1

144591 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1250-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1250-1

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-May/002046.html

SuSE SLED 12 SP1
x86_64
java-1_7_0-openjdk-headless-1.7.0.101-30.1
java-1_7_0-openjdk-debugsource-1.7.0.101-30.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-1.7.0.101-30.1

SuSE SLED 12
x86_64
java-1_7_0-openjdk-headless-1.7.0.101-30.1
java-1_7_0-openjdk-debugsource-1.7.0.101-30.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-1.7.0.101-30.1

SuSE SLES 12 SP1
x86_64
java-1_7_0-openjdk-headless-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-demo-1.7.0.101-30.1
java-1_7_0-openjdk-debugsource-1.7.0.101-30.1
java-1_7_0-openjdk-devel-1.7.0.101-30.1
java-1_7_0-openjdk-headless-1.7.0.101-30.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.101-30.1

java-1_7_0-openjdk-1.7.0.101-30.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-debuginfo-1.7.0.101-30.1

SuSE SLES 12
x86_64
java-1_7_0-openjdk-headless-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-demo-1.7.0.101-30.1
java-1_7_0-openjdk-debugsource-1.7.0.101-30.1
java-1_7_0-openjdk-devel-1.7.0.101-30.1
java-1_7_0-openjdk-headless-1.7.0.101-30.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-1.7.0.101-30.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.101-30.1
java-1_7_0-openjdk-debuginfo-1.7.0.101-30.1

160096 - CentOS 6, 7 CESA-2016-0726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
CESA-2016-0726

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021865.html
http://lists.centos.org/pipermail/centos-announce/2016-May/021866.html

CentOS 7
x86_64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2

i686
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2

CentOS 6
x86_64
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

i686

ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

160097 - CentOS 5, 6, 7 CESA-2016-0723 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
CESA-2016-0723

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021862.html
http://lists.centos.org/pipermail/centos-announce/2016-May/021861.html
http://lists.centos.org/pipermail/centos-announce/2016-May/021863.html

CentOS 6
x86_64
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7

i686
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7

CentOS 7
x86_64
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2

CentOS 5
x86_64
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

i386
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11

java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

160098 - CentOS 7 CESA-2016-0722 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
CESA-2016-0722

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-May/021860.html

CentOS 7
x86_64
openssl-devel-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-static-1.0.1e-51.el7_2.5

i686
openssl-devel-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-static-1.0.1e-51.el7_2.5

163073 - Oracle Enterprise Linux ELSA-2016-0723 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
ELSA-2016-0723

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006017.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006018.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006016.html

OEL6
x86_64
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7

java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7

i386
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7

OEL5
x86_64
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.0.1.el5_11

i386
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.0.1.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.0.1.el5_11

OEL7
x86_64
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2

163077 - Oracle Enterprise Linux ELSA-2016-0726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
ELSA-2016-0726

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006021.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006020.html

OEL7
x86_64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2

ImageMagick-c++-6.7.8.9-13.el7_2

OEL6
x86_64
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

i386
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

163078 - Oracle Enterprise Linux ELSA-2016-0722 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
ELSA-2016-0722

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006014.html

OEL7
x86_64
openssl-devel-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-static-1.0.1e-51.el7_2.5

174953 - Scientific Linux Security ERRATA Critical: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1605-1206)

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1605-1206)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=1206

SL5
x86_64
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

i386
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el5_11
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el5_11

SL7
x86_64
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el7_2
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el7_2

SL6
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

i386
java-1.6.0-openjdk-javadoc-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-devel-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-demo-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-src-1.6.0.39-1.13.11.0.el6_7
java-1.6.0-openjdk-1.6.0.39-1.13.11.0.el6_7

174955 - Scientific Linux Security ERRATA Important: openssl on SL7.x x86_64 (1605-778)

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: openssl on SL7.x x86_64 (1605-778)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=778

SL7
x86_64
openssl-static-1.0.1e-51.el7_2.5
openssl-debuginfo-1.0.1e-51.el7_2.5
openssl-libs-1.0.1e-51.el7_2.5
openssl-1.0.1e-51.el7_2.5
openssl-perl-1.0.1e-51.el7_2.5
openssl-devel-1.0.1e-51.el7_2.5

174956 - Scientific Linux Security ERRATA Important: ImageMagick on SL6.x, SL7.x i386/x86_64 (1605-1966)

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: ImageMagick on SL6.x, SL7.x i386/x86_64 (1605-1966)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=1966

SL7
x86_64
ImageMagick-6.7.8.9-13.el7_2
ImageMagick-debuginfo-6.7.8.9-13.el7_2
ImageMagick-c++-devel-6.7.8.9-13.el7_2
ImageMagick-perl-6.7.8.9-13.el7_2
ImageMagick-devel-6.7.8.9-13.el7_2
ImageMagick-doc-6.7.8.9-13.el7_2
ImageMagick-c++-6.7.8.9-13.el7_2

SL6
x86_64
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

i386
ImageMagick-doc-6.7.2.7-4.el6_7
ImageMagick-perl-6.7.2.7-4.el6_7
ImageMagick-devel-6.7.2.7-4.el6_7
ImageMagick-debuginfo-6.7.2.7-4.el6_7
ImageMagick-6.7.2.7-4.el6_7
ImageMagick-c++-devel-6.7.2.7-4.el6_7
ImageMagick-c++-6.7.2.7-4.el6_7

181944 - FreeBSD ImageMagick Multiple Vulnerabilities (0d724b05-687f-4527-9c03-af34d3b094ec)

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

Risk Level: High

CVE: CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718

Description

The scan detected that the host is missing the following update:
ImageMagick -- multiple vulnerabilities (0d724b05-687f-4527-9c03-af34d3b094ec)

Observation

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

http://www.vuxml.org/freebsd/0d724b05-687f-4527-9c03-af34d3b094ec.html

Affected packages:
ImageMagick < 6.9.3.9_1,1
ImageMagick-nox11 < 6.9.3.9_1,1
7.0.0.0.b20150715 <= ImageMagick7 < 7.0.1.0_1
7.0.0.0.b20150715 <= ImageMagick7-nox11 < 7.0.1.0_1

185262 - Ubuntu Linux 12.04 USN-2972-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

The scan detected that the host is missing the following update:
USN-2972-1

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-May/003418.html

Ubuntu 12.04

icedtea-6-jre-cacao_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-source_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-jre-zero_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-jre-lib_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-jdk_6b39-1.13.11-0ubuntu0.12.04.1
icedtea-6-jre-jamvm_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-jre_6b39-1.13.11-0ubuntu0.12.04.1
openjdk-6-jre-headless_6b39-1.13.11-0ubuntu0.12.04.1

185267 - Ubuntu Linux 12.04 USN-2967-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-1805, CVE-2015-7515, CVE-2015-7566, CVE-2015-7833, CVE-2015-8767, CVE-2015-8812, CVE-2016-0723, CVE-2016-0774, CVE-2016-0821, CVE-2016-2069, 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

Description

The scan detected that the host is missing the following update:
USN-2967-2

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-May/003410.html

Ubuntu 12.04

linux-image-3.2.0-1480-omap4_3.2.0-1480.106

185273 - Ubuntu Linux 12.04 USN-2967-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-1805, CVE-2015-7515, CVE-2015-7566, CVE-2015-7833, CVE-2015-8767, CVE-2015-8812, CVE-2016-0723, CVE-2016-0774, CVE-2016-0821, CVE-2016-2069, 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

Description

The scan detected that the host is missing the following update:
USN-2967-1

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-May/003409.html

Ubuntu 12.04

linux-image-3.2.0-102-generic-pae_3.2.0-102.142
linux-image-3.2.0-102-omap_3.2.0-102.142
linux-image-3.2.0-102-virtual_3.2.0-102.142
linux-image-3.2.0-102-highbank_3.2.0-102.142
linux-image-3.2.0-102-generic_3.2.0-102.142
linux-image-3.2.0-102-powerpc64-smp_3.2.0-102.142
linux-image-3.2.0-102-powerpc-smp_3.2.0-102.142

190626 - Fedora Linux 24 FEDORA-2016-1411324654 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1411324654

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183607.html

Fedora Core 24

openssl-1.0.2h-1.fc24

190629 - Fedora Linux 22 FEDORA-2016-1e39d934ed Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1e39d934ed

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184605.html

Fedora Core 22

openssl-1.0.1k-15.fc22

20063 - Oracle JRockit Critical Patch Update April 2016

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

Risk Level: High

CVE: CVE-2016-0695, CVE-2016-3425, CVE-2016-3427

Description

Multiple vulnerabilities are present in some versions of Oracle JRockit.

Observation

Oracle JRockit is a Java Virtual Machine (JVM).

Multiple vulnerabilities are present in some versions of Oracle JRockit. The flaws lie in the Oracle JRockit components. Successful exploitation by a remote attacker could affect confidentiality, integrity, and availability.

20067 - (HT206338) Apple Xcode Git Heap Buffer Overflow Vulnerabilities

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-2315, CVE-2016-2324

Description

Multiple vulnerabilities are present in some versions of Apple Xcode.

Observation

Apple Xcode is a development framework for MAC OS X and iOS devices.

Multiple vulnerabilities are present in some versions of Apple Xcode. The flaws lie in Git component. Successful exploitation could allow an attacker to execute remote code.

20074 - (APSB16-15) Vulnerabilities in Adobe Flash Player

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

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117

Description

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

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic or memory issues. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-15 resolves the issues. The target system is missing this update.

20078 - (APSB16-15) Vulnerabilities in Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1096, CVE-2016-1097, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1101, CVE-2016-1102, CVE-2016-1103, CVE-2016-1104, CVE-2016-1105, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, CVE-2016-4109, CVE-2016-4110, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4116, CVE-2016-4117

Description

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

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic or memory issues. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-15 resolves the issues. The target system is missing this update.

190597 - Fedora Linux 22 FEDORA-2016-338a7e9925 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523, CVE-2016-1526

Description

The scan detected that the host is missing the following update:
FEDORA-2016-338a7e9925

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184623.html

Fedora Core 22

graphite2-1.3.6-1.fc22

19994 - Cisco Adaptive Security Appliance Software DHCPv6 Relay Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1367

Description

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software.

Observation

Cisco Adaptive Security Appliance Software is the operating system used in Cisco ASA device.

A denial of service vulnerability is present in some versions of Cisco Adaptive Security Appliance Software. The flaw lies in processing of DHCPv6 packets. Successful exploitation could allow an attacker to cause denial of service condition.

20072 - Opera Multiple Vulnerabilities Prior To 37

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Opera.

Observation

Opera is a popular web browser.

Multiple vulnerabilities are present in some versions of Opera. The flaws lie in Chromium/Blink used by Opera. Successful exploitation could allow an attacker to execute arbitrary code.

19996 - (HPSBUX03583) HP-UX BIND Service Named Remote Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-1285, CVE-2016-1286

Description

Multiple vulnerabilities are present in some versions of HP-UX BIND.

Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX BIND. The flaws are due to improper handling of signature records and control channel input. Successful exploitation could allow an attacker to cause a denial of service.

19998 - (JSA10739) Juniper Junos CLI Multiple Privilege Escalation Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1271

Description

A privilege escalation vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper switches and routers.

A privilege escalation vulnerability is present in some versions of Juniper Junos. The flaw could be exploited by certain combinations of Junos OS CLI commands and arguments. Successful exploitation could allow root access to the operating system.

20004 - Google Chrome Multiple Vulnerabilities Prior To 50.0.2661.94

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

Risk Level: High

CVE: CVE-2016-1660, CVE-2016-1661, CVE-2016-1662, CVE-2016-1663, CVE-2016-1664, CVE-2016-1665, CVE-2016-1666

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code, obtain sensitive information or possibly cause other unspecified impact.

20005 - Google Chrome Multiple Vulnerabilities Prior To 50.0.2661.94

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1660, CVE-2016-1661, CVE-2016-1662, CVE-2016-1663, CVE-2016-1664, CVE-2016-1665, CVE-2016-1666

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code, obtain sensitive information or possibly cause other unspecified impact.

20060 - (JSA10736) Juniper Junos Manipulating TCP Timestamps Resource Exhaustion Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1269

Description

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

Observation

Juniper Junos is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos. The flaw lies in handling of TCP packets. Successful exploitation could allow an attacker to cause denial of service.

20068 - (JSA10725) Juniper Junos Op Script Op URL Option Race Condition Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1264

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in the Op script Op URL option. Successful exploitation could allow an attacker to escalate privileges.

132233 - Oracle VM OVMSA-2016-0046 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805, CVE-2015-8767, CVE-2016-0774

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0046

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000457.html

OVM3.3
x86_64
kernel-uek-firmware-3.8.13-118.6.1.el6uek
kernel-uek-3.8.13-118.6.1.el6uek

141181 - Red Hat Enterprise Linux RHSA-2016-0760 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1571, CVE-2014-3538, CVE-2014-3587, CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9620, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
RHSA-2016-0760

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0760.html

RHEL6D
x86_64
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

i386
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

RHEL6S
i386
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

x86_64
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

RHEL6WS
x86_64
file-debuginfo-5.04-30.el6
file-5.04-30.el6
file-libs-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

i386
file-debuginfo-5.04-30.el6
file-5.04-30.el6

file-libs-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

141182 - Red Hat Enterprise Linux RHSA-2016-0724 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
RHSA-2016-0724

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0724.html

RHEL7D
x86_64
qemu-kvm-debuginfo-1.5.3-105.el7_2.4
libcacard-1.5.3-105.el7_2.4
qemu-kvm-1.5.3-105.el7_2.4
qemu-kvm-tools-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4
qemu-kvm-common-1.5.3-105.el7_2.4

RHEL7S
ppc64
qemu-kvm-debuginfo-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
libcacard-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4

RHEL7WS
x86_64
qemu-kvm-debuginfo-1.5.3-105.el7_2.4
libcacard-1.5.3-105.el7_2.4
qemu-kvm-1.5.3-105.el7_2.4
qemu-kvm-tools-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4
qemu-kvm-common-1.5.3-105.el7_2.4

141183 - Red Hat Enterprise Linux RHSA-2016-0997 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
RHSA-2016-0997

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0997.html

RHEL6D
x86_64
qemu-kvm-tools-0.12.1.2-2.491.el6_8.1
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1
qemu-kvm-0.12.1.2-2.491.el6_8.1
qemu-img-0.12.1.2-2.491.el6_8.1

i386
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1

RHEL6S
i386
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1

x86_64
qemu-kvm-tools-0.12.1.2-2.491.el6_8.1
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1
qemu-kvm-0.12.1.2-2.491.el6_8.1
qemu-img-0.12.1.2-2.491.el6_8.1

RHEL6WS
x86_64
qemu-kvm-tools-0.12.1.2-2.491.el6_8.1
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1
qemu-kvm-0.12.1.2-2.491.el6_8.1
qemu-img-0.12.1.2-2.491.el6_8.1

i386
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1

160099 - CentOS 7 CESA-2016-0724 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
CESA-2016-0724

Observation

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

For more information see:

http://lists.centos.org/pipermail/centos-announce/2016-May/021864.html

CentOS 7
x86_64
libcacard-1.5.3-105.el7_2.4
qemu-kvm-1.5.3-105.el7_2.4
qemu-kvm-tools-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4
qemu-kvm-common-1.5.3-105.el7_2.4

i686
libcacard-devel-1.5.3-105.el7_2.4
libcacard-1.5.3-105.el7_2.4

163076 - Oracle Enterprise Linux ELSA-2016-0724 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
ELSA-2016-0724

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006019.html

OEL7
x86_64
libcacard-1.5.3-105.el7_2.4
qemu-kvm-1.5.3-105.el7_2.4
qemu-kvm-tools-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4
qemu-kvm-common-1.5.3-105.el7_2.4

174954 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1605-1638)

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1605-1638)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1605&L=scientific-linux-errata&F=&S=&P=1638

SL7
x86_64
qemu-kvm-debuginfo-1.5.3-105.el7_2.4
libcacard-1.5.3-105.el7_2.4
qemu-kvm-1.5.3-105.el7_2.4
qemu-kvm-tools-1.5.3-105.el7_2.4
libcacard-tools-1.5.3-105.el7_2.4
qemu-img-1.5.3-105.el7_2.4
libcacard-devel-1.5.3-105.el7_2.4
qemu-kvm-common-1.5.3-105.el7_2.4

185261 - Ubuntu Linux 15.10 USN-2971-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7515, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2971-3

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-May/003417.html

Ubuntu 15.10

linux-image-4.2.0-1029-raspi2_4.2.0-1029.37

185263 - Ubuntu Linux 16.04 USN-2965-4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3689, CVE-2016-3951, CVE-2016-3955, CVE-2016-4557

Description

The scan detected that the host is missing the following update:
USN-2965-4

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-May/003407.html

Ubuntu 16.04

linux-image-4.4.0-1013-snapdragon_4.4.0-1013.14

185264 - Ubuntu Linux 16.04 USN-2965-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3689, CVE-2016-3951, CVE-2016-3955, CVE-2016-4557

Description

The scan detected that the host is missing the following update:
USN-2965-1

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-May/003404.html

Ubuntu 16.04

linux-image-4.4.0-22-powerpc64-smp_4.4.0-22.39
linux-image-4.4.0-22-lowlatency_4.4.0-22.39
linux-image-4.4.0-22-generic-lpae_4.4.0-22.39
linux-image-4.4.0-22-generic_4.4.0-22.39
linux-image-4.4.0-22-powerpc64-emb_4.4.0-22.39
linux-image-4.4.0-22-powerpc-e500mc_4.4.0-22.39
linux-image-4.4.0-22-powerpc-smp_4.4.0-22.39

185265 - Ubuntu Linux 12.04 USN-2968-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805, CVE-2015-7515, CVE-2015-8830, CVE-2016-0774, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2968-2

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-May/003412.html

Ubuntu 12.04

linux-image-3.13.0-86-generic_3.13.0-86.130~precise1
linux-image-3.13.0-86-generic-lpae_3.13.0-86.130~precise1

185266 - Ubuntu Linux 14.04 USN-2968-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1805, CVE-2015-7515, CVE-2015-8830, CVE-2016-0774, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2968-1

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-May/003411.html

Ubuntu 14.04

linux-image-3.13.0-86-powerpc-e500mc_3.13.0-86.130
linux-image-3.13.0-86-powerpc64-emb_3.13.0-86.130
linux-image-3.13.0-86-powerpc-smp_3.13.0-86.130
linux-image-3.13.0-86-generic_3.13.0-86.130
linux-image-3.13.0-86-powerpc-e500_3.13.0-86.130
linux-image-3.13.0-86-generic-lpae_3.13.0-86.130
linux-image-3.13.0-86-lowlatency_3.13.0-86.130
linux-image-3.13.0-86-powerpc64-smp_3.13.0-86.130

185268 - Ubuntu Linux 16.04 USN-2965-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3689, CVE-2016-3951, CVE-2016-3955, CVE-2016-4557

Description

The scan detected that the host is missing the following update:
USN-2965-3

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-May/003406.html

Ubuntu 16.04

linux-image-4.4.0-1010-raspi2_4.4.0-1010.12

185269 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2966-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325, CVE-2016-1907, CVE-2016-1908, CVE-2016-3115

Description

The scan detected that the host is missing the following update:
USN-2966-1

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-May/003408.html

Ubuntu 12.04

openssh-server_5.9p1-5ubuntu1.9

Ubuntu 15.10

openssh-server_6.9p1-2ubuntu0.2

Ubuntu 14.04

openssh-server_6.6p1-2ubuntu2.7

185270 - Ubuntu Linux 14.04 USN-2971-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7515, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2971-2

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-May/003416.html

Ubuntu 14.04

linux-image-4.2.0-36-powerpc-smp_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-powerpc64-emb_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-powerpc64-smp_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-powerpc-e500mc_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-lowlatency_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-generic_4.2.0-36.41~14.04.1
linux-image-4.2.0-36-generic-lpae_4.2.0-36.41~14.04.1

185271 - Ubuntu Linux 14.04 USN-2969-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7515, CVE-2015-8830, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3138, CVE-2016-3156, CVE-2016-3157

Description

The scan detected that the host is missing the following update:
USN-2969-1

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-May/003413.html

Ubuntu 14.04

linux-image-3.16.0-71-powerpc64-smp_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-generic-lpae_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-powerpc64-emb_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-powerpc-smp_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-lowlatency_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-powerpc-e500mc_3.16.0-71.91~14.04.1
linux-image-3.16.0-71-generic_3.16.0-71.91~14.04.1

185272 - Ubuntu Linux 14.04 USN-2965-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-2847, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3689, CVE-2016-3951, CVE-2016-3955, CVE-2016-4557

Description

The scan detected that the host is missing the following update:
USN-2965-2

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-May/003405.html

Ubuntu 14.04

linux-image-4.4.0-22-lowlatency_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-powerpc64-smp_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-generic_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-powerpc64-emb_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-powerpc-smp_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-powerpc-e500mc_4.4.0-22.39~14.04.1
linux-image-4.4.0-22-generic-lpae_4.4.0-22.39~14.04.1

185274 - Ubuntu Linux 14.04 USN-2970-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7515, CVE-2015-8830, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2970-1

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-May/003414.html

Ubuntu 14.04

linux-image-3.19.0-59-generic-lpae_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-generic_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-powerpc-e500mc_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-powerpc-smp_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-powerpc64-emb_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-lowlatency_3.19.0-59.65~14.04.1
linux-image-3.19.0-59-powerpc64-smp_3.19.0-59.65~14.04.1

185275 - Ubuntu Linux 15.10 USN-2971-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7515, CVE-2016-0821, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3689

Description

The scan detected that the host is missing the following update:
USN-2971-1

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-May/003415.html

Ubuntu 15.10

linux-image-4.2.0-36-generic_4.2.0-36.41
linux-image-4.2.0-36-powerpc64-smp_4.2.0-36.41
linux-image-4.2.0-36-generic-lpae_4.2.0-36.41
linux-image-4.2.0-36-lowlatency_4.2.0-36.41
linux-image-4.2.0-36-powerpc-e500mc_4.2.0-36.41
linux-image-4.2.0-36-powerpc-smp_4.2.0-36.41
linux-image-4.2.0-36-powerpc64-emb_4.2.0-36.41

190604 - Fedora Linux 24 FEDORA-2016-48e72b7bc5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3960, CVE-2016-4001, CVE-2016-4002, CVE-2016-4037

Description

The scan detected that the host is missing the following update:
FEDORA-2016-48e72b7bc5

Observation

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

For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184209.html

Fedora Core 24

xen-4.6.1-6.fc24

190608 - Fedora Linux 23 FEDORA-2016-68abc0be35 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779, CVE-2016-1234, CVE-2016-3075

Description

The scan detected that the host is missing the following update:
FEDORA-2016-68abc0be35

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184626.html

Fedora Core 23

glibc-2.22-15.fc23

190612 - Fedora Linux 24 FEDORA-2016-821f013cb1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2774

Description

The scan detected that the host is missing the following update:
FEDORA-2016-821f013cb1

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183640.html

Fedora Core 24

dhcp-4.3.4-1.fc24

190614 - Fedora Linux 24 FEDORA-2016-852a39e085 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2665, CVE-2015-4342, CVE-2015-4454

Description

The scan detected that the host is missing the following update:
FEDORA-2016-852a39e085

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183919.html

Fedora Core 24

cacti-0.8.8g-1.fc24

190620 - Fedora Linux 24 FEDORA-2016-0c57b12c7b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3074

Description

The scan detected that the host is missing the following update:
FEDORA-2016-0c57b12c7b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183724.html

Fedora Core 24

gd-2.1.1-7.fc24

20058 - (SYM16-005) Symantec Messaging Gateway Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-2203, CVE-2016-2204

Description

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway.

Observation

Symantec Messaging Gateway is an email security solution.

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or escalate privilege.

20062 - (JSA10734) Juniper Junos OpenSSH Client Information Leak and Buffer Overflow Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-0777, CVE-2016-0778

Description

Two vulnerabilities are present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

Two vulnerabilities are present in some versions of Juniper Junos. The flaws lie in the OpenSSH client. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or possibly have unspecified other impact.

20071 - WordPress Multiple Vulnerabilities Prior To 4.5.2

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blog application.

Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components. Successful exploitation could allow an attacker to inject and execute arbitrary JavaScript code in the context of the victim's browser session, or launch a Same Origin Method Execution attack.

130491 - Debian Linux 8.0 DSA-3574-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1541

Description

The scan detected that the host is missing the following update:
DSA-3574-1

Observation

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

http://www.debian.org/security/2016/dsa-3574

Debian 8.0
all
libarchive13_3.1.2-11+deb8u1
bsdcpio_3.1.2-11+deb8u1
bsdtar_3.1.2-11+deb8u1
libarchive-dev_3.1.2-11+deb8u1

130492 - Debian Linux 8.0 DSA-3570-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3105

Description

The scan detected that the host is missing the following update:
DSA-3570-1

Observation

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

http://www.debian.org/security/2016/dsa-3570

Debian 8.0
all
mercurial_3.1.2-2+deb8u3

141187 - Red Hat Enterprise Linux RHSA-2016-0741 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5352, CVE-2015-6563, CVE-2015-6564, CVE-2016-1908

Description

The scan detected that the host is missing the following update:
RHSA-2016-0741

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0741.html

RHEL6D
x86_64
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

i386
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

RHEL6S
i386
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6

openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

x86_64
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

RHEL6WS
x86_64
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6
openssh-server-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6

i386
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6
openssh-server-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6

141188 - Red Hat Enterprise Linux RHSA-2016-0855 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5313, CVE-2013-4312, CVE-2014-7842, CVE-2014-8134, CVE-2015-5156, CVE-2015-7509, CVE-2015-8215, CVE-2015-8324, CVE-2015-8543

Description

The scan detected that the host is missing the following update:
RHSA-2016-0855

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0855.html

RHEL6D
i386
kernel-devel-2.6.32-642.el6
python-perf-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
perf-debuginfo-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6

noarch
kernel-abi-whitelists-2.6.32-642.el6
kernel-firmware-2.6.32-642.el6
kernel-doc-2.6.32-642.el6

x86_64
perf-debuginfo-2.6.32-642.el6
python-perf-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
kernel-debuginfo-common-x86_64-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6
kernel-devel-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6

RHEL6S
i386
kernel-devel-2.6.32-642.el6
python-perf-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
perf-debuginfo-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6

noarch
kernel-abi-whitelists-2.6.32-642.el6
kernel-firmware-2.6.32-642.el6
kernel-doc-2.6.32-642.el6

x86_64
perf-debuginfo-2.6.32-642.el6
python-perf-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
kernel-debuginfo-common-x86_64-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6
kernel-devel-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6

RHEL6WS
i386
kernel-devel-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6

kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
perf-debuginfo-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6

noarch
kernel-abi-whitelists-2.6.32-642.el6
kernel-firmware-2.6.32-642.el6
kernel-doc-2.6.32-642.el6

x86_64
kernel-devel-2.6.32-642.el6
perf-2.6.32-642.el6
kernel-debuginfo-2.6.32-642.el6
kernel-debuginfo-common-i686-2.6.32-642.el6
kernel-headers-2.6.32-642.el6
kernel-debug-devel-2.6.32-642.el6
perf-debuginfo-2.6.32-642.el6
kernel-debug-2.6.32-642.el6
kernel-2.6.32-642.el6
kernel-debuginfo-common-x86_64-2.6.32-642.el6
python-perf-debuginfo-2.6.32-642.el6
kernel-debug-debuginfo-2.6.32-642.el6

141189 - Red Hat Enterprise Linux RHSA-2016-0778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5234, CVE-2015-5235

Description

The scan detected that the host is missing the following update:
RHSA-2016-0778

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0778.html

RHEL6D
i386
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

noarch
icedtea-web-javadoc-1.6.2-1.el6

x86_64
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

RHEL6S
i386

icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

noarch
icedtea-web-javadoc-1.6.2-1.el6

x86_64
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

RHEL6WS
x86_64
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

i386
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

144586 - SuSE SLES 11 SP4 SUSE-SU-2016:1259-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3247, CVE-2015-5260, CVE-2015-5261

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1259-1

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-May/002048.html

SuSE SLES 11 SP4
x86_64
libspice-server1-0.12.4-5.1

i586
libspice-server1-0.12.4-5.1

181942 - FreeBSD libarchive RCE Vulnerability (2b4c8e1f-1609-11e6-b55e-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2016-1541

Description

The scan detected that the host is missing the following update:
libarchive -- RCE vulnerability (2b4c8e1f-1609-11e6-b55e-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/2b4c8e1f-1609-11e6-b55e-b499baebfeaf.html

Affected packages:
libarchive < 3.2.0,1

190605 - Fedora Linux 22 FEDORA-2016-7b40eb9e29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3455, CVE-2015-5400, CVE-2016-2571, CVE-2016-2572

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7b40eb9e29

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183597.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183598.html

Fedora Core 22

squid-3.5.10-1.fc22
libecap-1.0.0-1.fc22

20061 - IBM AIX OpenSSH Multiple Vulnerabilities (openssh_advisory8)

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

Risk Level: Medium

CVE: CVE-2016-1908, CVE-2016-3115

Description

Multiple vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in OpenSSH. Successful exploitation could allow a remote attacker to bypass certain security restrictions, or inject arbitrary commands.

20066 - (HPSBMU03573) HPE System Management Homepage Remote Disclosure of Information Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-0800

Description

An information disclosure vulnerability is present in some versions of HP System Management Homepage.

Observation

HP System Management Homepage is a web-based interface that consolidates and simplifies the management of individual ProLiant

and Integrity servers.

An information disclosure vulnerability is present in some versions of HP System Management Homepage. The flaw lies in SSLv2 protocol. Successful exploitation could allow an attacker to disclose information.

132232 - Oracle VM OVMSA-2016-0047 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8767

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0047

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-May/000458.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-37.2.2.el6uek
kernel-uek-4.1.12-37.2.2.el6uek

141186 - Red Hat Enterprise Linux RHSA-2016-0780 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7977, CVE-2015-7978

Description

The scan detected that the host is missing the following update:
RHSA-2016-0780

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-0780.html

RHEL6D
i386
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

noarch
ntp-doc-4.2.6p5-10.el6

x86_64
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6

ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

RHEL6S
i386
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

noarch
ntp-doc-4.2.6p5-10.el6

x86_64
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

RHEL6WS
x86_64
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6

i386
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6

163072 - Oracle Enterprise Linux ELSA-2016-3553 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8767

Description

The scan detected that the host is missing the following update:
ELSA-2016-3553

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006004.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006005.html

OEL5
x86_64
kernel-uek-devel-2.6.32-400.37.16.el5uek
kernel-uek-firmware-2.6.32-400.37.16.el5uek
ofa-2.6.32-400.37.16.el5uekdebug-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.16.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.37.16.el5uek
kernel-uek-debug-2.6.32-400.37.16.el5uek
ofa-2.6.32-400.37.16.el5uek-1.5.1-4.0.58
kernel-uek-doc-2.6.32-400.37.16.el5uek
mlnx_en-2.6.32-400.37.16.el5uekdebug-1.5.7-2

kernel-uek-2.6.32-400.37.16.el5uek

i386
kernel-uek-devel-2.6.32-400.37.16.el5uek
kernel-uek-debug-2.6.32-400.37.16.el5uek
ofa-2.6.32-400.37.16.el5uekdebug-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.16.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.37.16.el5uek
ofa-2.6.32-400.37.16.el5uek-1.5.1-4.0.58
kernel-uek-doc-2.6.32-400.37.16.el5uek
mlnx_en-2.6.32-400.37.16.el5uekdebug-1.5.7-2
kernel-uek-2.6.32-400.37.16.el5uek
kernel-uek-firmware-2.6.32-400.37.16.el5uek

OEL6
x86_64
mlnx_en-2.6.32-400.37.16.el6uek-1.5.7-0.1
kernel-uek-debug-devel-2.6.32-400.37.16.el6uek
kernel-uek-firmware-2.6.32-400.37.16.el6uek
ofa-2.6.32-400.37.16.el6uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.16.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.37.16.el6uekdebug-1.5.1-4.0.58
kernel-uek-2.6.32-400.37.16.el6uek
kernel-uek-devel-2.6.32-400.37.16.el6uek
kernel-uek-debug-2.6.32-400.37.16.el6uek
kernel-uek-doc-2.6.32-400.37.16.el6uek

i386
mlnx_en-2.6.32-400.37.16.el6uek-1.5.7-0.1
kernel-uek-debug-devel-2.6.32-400.37.16.el6uek
kernel-uek-firmware-2.6.32-400.37.16.el6uek
ofa-2.6.32-400.37.16.el6uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.16.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.37.16.el6uekdebug-1.5.1-4.0.58
kernel-uek-2.6.32-400.37.16.el6uek
kernel-uek-devel-2.6.32-400.37.16.el6uek
kernel-uek-debug-2.6.32-400.37.16.el6uek
kernel-uek-doc-2.6.32-400.37.16.el6uek

163074 - Oracle Enterprise Linux ELSA-2016-3551 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8767

Description

The scan detected that the host is missing the following update:
ELSA-2016-3551

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006001.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006000.html

OEL7
x86_64

kernel-uek-devel-3.8.13-118.6.1.el7uek
kernel-uek-firmware-3.8.13-118.6.1.el7uek
kernel-uek-debug-devel-3.8.13-118.6.1.el7uek
dtrace-modules-3.8.13-118.6.1.el7uek-0.4.5-3.el7
kernel-uek-doc-3.8.13-118.6.1.el7uek
kernel-uek-3.8.13-118.6.1.el7uek
kernel-uek-debug-3.8.13-118.6.1.el7uek

OEL6
x86_64
kernel-uek-debug-devel-3.8.13-118.6.1.el6uek
dtrace-modules-3.8.13-118.6.1.el6uek-0.4.5-3.el6
kernel-uek-doc-3.8.13-118.6.1.el6uek
kernel-uek-firmware-3.8.13-118.6.1.el6uek
kernel-uek-3.8.13-118.6.1.el6uek
kernel-uek-debug-3.8.13-118.6.1.el6uek
kernel-uek-devel-3.8.13-118.6.1.el6uek

163075 - Oracle Enterprise Linux ELSA-2016-3554 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8767

Description

The scan detected that the host is missing the following update:
ELSA-2016-3554

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006006.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006007.html

OEL7
x86_64
kernel-uek-devel-4.1.12-37.2.2.el7uek
kernel-uek-doc-4.1.12-37.2.2.el7uek
kernel-uek-debug-4.1.12-37.2.2.el7uek
kernel-uek-4.1.12-37.2.2.el7uek
kernel-uek-debug-devel-4.1.12-37.2.2.el7uek
kernel-uek-firmware-4.1.12-37.2.2.el7uek
dtrace-modules-4.1.12-37.2.2.el7uek-0.5.2-1.el7

OEL6
x86_64
kernel-uek-doc-4.1.12-37.2.2.el6uek
kernel-uek-debug-4.1.12-37.2.2.el6uek
kernel-uek-debug-devel-4.1.12-37.2.2.el6uek
dtrace-modules-4.1.12-37.2.2.el6uek-0.5.2-1.el6
kernel-uek-devel-4.1.12-37.2.2.el6uek
kernel-uek-firmware-4.1.12-37.2.2.el6uek
kernel-uek-4.1.12-37.2.2.el6uek

163079 - Oracle Enterprise Linux ELSA-2016-3552 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8767

Description

The scan detected that the host is missing the following update:
ELSA-2016-3552

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-May/006003.html
http://oss.oracle.com/pipermail/el-errata/2016-May/006002.html

OEL5
x86_64
kernel-uek-debug-2.6.39-400.278.2.el5uek
kernel-uek-debug-devel-2.6.39-400.278.2.el5uek
kernel-uek-devel-2.6.39-400.278.2.el5uek
kernel-uek-2.6.39-400.278.2.el5uek
kernel-uek-doc-2.6.39-400.278.2.el5uek
kernel-uek-firmware-2.6.39-400.278.2.el5uek

i386
kernel-uek-debug-2.6.39-400.278.2.el5uek
kernel-uek-debug-devel-2.6.39-400.278.2.el5uek
kernel-uek-devel-2.6.39-400.278.2.el5uek
kernel-uek-firmware-2.6.39-400.278.2.el5uek
kernel-uek-2.6.39-400.278.2.el5uek
kernel-uek-doc-2.6.39-400.278.2.el5uek

OEL6
x86_64
kernel-uek-doc-2.6.39-400.278.2.el6uek
kernel-uek-2.6.39-400.278.2.el6uek
kernel-uek-firmware-2.6.39-400.278.2.el6uek
kernel-uek-devel-2.6.39-400.278.2.el6uek
kernel-uek-debug-2.6.39-400.278.2.el6uek
kernel-uek-debug-devel-2.6.39-400.278.2.el6uek

i386
kernel-uek-doc-2.6.39-400.278.2.el6uek
kernel-uek-2.6.39-400.278.2.el6uek
kernel-uek-firmware-2.6.39-400.278.2.el6uek
kernel-uek-devel-2.6.39-400.278.2.el6uek
kernel-uek-debug-2.6.39-400.278.2.el6uek
kernel-uek-debug-devel-2.6.39-400.278.2.el6uek

181941 - FreeBSD perl5 Taint Mechanism Bypass Vulnerability (d9f99491-1656-11e6-94fa-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2016-2381

Description

The scan detected that the host is missing the following update:
perl5 -- taint mechanism bypass vulnerability (d9f99491-1656-11e6-94fa-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/d9f99491-1656-11e6-94fa-002590263bf5.html

Affected packages:
perl5 < 5.18.4_21
5.20.0 <= perl5 < 5.20.3_12
5.22.0 <= perl5 < 5.22.1_8
5.18.0 <= perl5.18 < 5.18.4_21
5.20.0 <= perl5.20 < 5.20.3_12
5.22.0 <= perl5.22 < 5.22.1_8

190621 - Fedora Linux 24 FEDORA-2016-08e5803496 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3115

Description

The scan detected that the host is missing the following update:
FEDORA-2016-08e5803496

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184264.html

Fedora Core 24

gsi-openssh-7.2p2-2.fc24

19997 - Cisco IOS ntp Subsystem Unauthorized Access Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-1384

Description

A vulnerability is present in some versions of Cisco IOS.

Observation

Cisco IOS is an operating system used in Cisco devices.

A vulnerability is present in some versions of Cisco IOS. The flaw is due to improper handling of certain ntp packets. Successful exploitation could allow an attacker to control the time of the affected device.

20065 - (JSA10730) Juniper Junos RPC Lazy Race Condition Privilege Escalation Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-1267

Description

A privilege escalation vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper devices.

A privilege escalation vulnerability is present in some versions of Juniper Junos. The flaw lies in the RPC functionality. Successful exploitation could allow an attacker to escalate privileges.

144588 - SuSE Linux 13.2 openSUSE-SU-2016:1264-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1264-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-05/msg00044.html

SuSE Linux 13.2
i586
subversion-1.8.16-2.26.1
subversion-debuginfo-1.8.16-2.26.1
subversion-python-debuginfo-1.8.16-2.26.1
subversion-perl-debuginfo-1.8.16-2.26.1
subversion-tools-1.8.16-2.26.1
subversion-tools-debuginfo-1.8.16-2.26.1
subversion-server-1.8.16-2.26.1
subversion-python-1.8.16-2.26.1
subversion-devel-1.8.16-2.26.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.8.16-2.26.1
subversion-python-ctypes-1.8.16-2.26.1
subversion-debugsource-1.8.16-2.26.1
libsvn_auth_kwallet-1-0-debuginfo-1.8.16-2.26.1
libsvn_auth_gnome_keyring-1-0-1.8.16-2.26.1
subversion-ruby-debuginfo-1.8.16-2.26.1
libsvn_auth_kwallet-1-0-1.8.16-2.26.1
subversion-perl-1.8.16-2.26.1
subversion-ruby-1.8.16-2.26.1
subversion-server-debuginfo-1.8.16-2.26.1

noarch
subversion-bash-completion-1.8.16-2.26.1

x86_64
subversion-1.8.16-2.26.1
subversion-debuginfo-1.8.16-2.26.1
subversion-python-debuginfo-1.8.16-2.26.1
subversion-perl-debuginfo-1.8.16-2.26.1

subversion-tools-1.8.16-2.26.1
subversion-tools-debuginfo-1.8.16-2.26.1
subversion-server-1.8.16-2.26.1
subversion-python-1.8.16-2.26.1
subversion-devel-1.8.16-2.26.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.8.16-2.26.1
subversion-python-ctypes-1.8.16-2.26.1
subversion-debugsource-1.8.16-2.26.1
libsvn_auth_kwallet-1-0-debuginfo-1.8.16-2.26.1
libsvn_auth_gnome_keyring-1-0-1.8.16-2.26.1
subversion-ruby-debuginfo-1.8.16-2.26.1
libsvn_auth_kwallet-1-0-1.8.16-2.26.1
subversion-perl-1.8.16-2.26.1
subversion-ruby-1.8.16-2.26.1
subversion-server-debuginfo-1.8.16-2.26.1

190592 - Fedora Linux 22 FEDORA-2016-373c063e79 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8839, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961

Description

The scan detected that the host is missing the following update:
FEDORA-2016-373c063e79

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183593.html

Fedora Core 22

kernel-4.4.8-200.fc22

190615 - Fedora Linux 22 FEDORA-2016-9851b69dbb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1926

Description

The scan detected that the host is missing the following update:
FEDORA-2016-9851b69dbb

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184477.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184478.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184476.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184475.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184479.html

Fedora Core 22

openvas-manager-6.0.8-2.fc22
openvas-scanner-5.0.5-3.fc22
openvas-libraries-8.0.7-2.fc22
openvas-gsa-6.0.10-3.fc22
openvas-cli-1.4.4-1.fc22

190617 - Fedora Linux 24 FEDORA-2016-20cc04ac50 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

Description

The scan detected that the host is missing the following update:
FEDORA-2016-20cc04ac50

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184545.html

Fedora Core 24

subversion-1.9.4-1.fc24

130487 - Debian Linux 8.0 DSA-3571-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4561

Description

The scan detected that the host is missing the following update:
DSA-3571-1

Observation

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

http://www.debian.org/security/2016/dsa-3571

Debian 8.0
all
ikiwiki_3.20141016.3

130488 - Debian Linux 8.0 DSA-3572-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1236

Description

The scan detected that the host is missing the following update:
DSA-3572-1

Observation

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

http://www.debian.org/security/2016/dsa-3572

Debian 8.0
all
websvn_2.3.3-1.2+deb8u2

130489 - Debian Linux 8.0 DSA-3573-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3710, CVE-2016-3712

Description

The scan detected that the host is missing the following update:
DSA-3573-1

Observation

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

http://www.debian.org/security/2016/dsa-3573

Debian 8.0
all
qemu_1:2.1+dfsg-12+deb8u6

130490 - Debian Linux 8.0 DSA-3569-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8312, CVE-2016-2860

Description

The scan detected that the host is missing the following update:
DSA-3569-1

Observation

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

http://www.debian.org/security/2016/dsa-3569

Debian 8.0
all
openafs-modules-dkms_1.6.9-2+deb8u5
libpam-openafs-kaserver_1.6.9-2+deb8u5
libafsauthent1_1.6.9-2+deb8u5

openafs-dbg_1.6.9-2+deb8u5
openafs-modules-source_1.6.9-2+deb8u5
openafs-client_1.6.9-2+deb8u5
openafs-fileserver_1.6.9-2+deb8u5
openafs-dbserver_1.6.9-2+deb8u5
openafs-kpasswd_1.6.9-2+deb8u5
openafs-krb5_1.6.9-2+deb8u5
libopenafs-dev_1.6.9-2+deb8u5
openafs-fuse_1.6.9-2+deb8u5
openafs-doc_1.6.9-2+deb8u5
libkopenafs1_1.6.9-2+deb8u5
libafsrpc1_1.6.9-2+deb8u5

181943 - FreeBSD squid Multiple Vulnerabilities (25e5205b-1447-11e6-9ead-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Description

The scan detected that the host is missing the following update:
squid -- multiple vulnerabilities (25e5205b-1447-11e6-9ead-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/25e5205b-1447-11e6-9ead-6805ca0b3d42.html

Affected packages:
3.0.0 <= squid < 3.5.18
4.0.0 <= squid-devel < 4.0.10

181945 - FreeBSD wordpress Multiple Vulnerabilities (3686917b-164d-11e6-94fa-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-4566, CVE-2016-4567

Description

The scan detected that the host is missing the following update:
wordpress -- multiple vulnerabilities (3686917b-164d-11e6-94fa-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/3686917b-164d-11e6-94fa-002590263bf5.html

Affected packages:
wordpress < 4.5.2,1
de-wordpress < 4.5.2
ja-wordpress < 4.5.2
ru-wordpress < 4.5.2
zh-wordpress-zh_CN < 4.5.2
zh-wordpress-zh_TW < 4.5.2

190589 - Fedora Linux 24 FEDORA-2016-13b4cae9df Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3720

Description

The scan detected that the host is missing the following update:
FEDORA-2016-13b4cae9df

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184561.html

Fedora Core 24

jackson-dataformat-xml-2.6.3-3.fc24

190590 - Fedora Linux 24 FEDORA-2016-7e287fa1e6 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-2016-7e287fa1e6

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184112.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184116.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184115.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184113.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184119.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184120.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184117.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184121.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184122.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184114.html
http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184118.html

Fedora Core 24

NetworkManager-vpnc-1.2.0-1.fc24
NetworkManager-ssh-1.2.0-1.fc24
network-manager-applet-1.2.0-1.fc24
NetworkManager-l2tp-1.2.0-1.fc24
NetworkManager-1.2.0-1.fc24
NetworkManager-openvpn-1.2.0-1.fc24
NetworkManager-libreswan-1.2.0-1.fc24

NetworkManager-fortisslvpn-1.2.0-1.fc24
NetworkManager-iodine-1.2.0-1.fc24
NetworkManager-openconnect-1.2.0-1.fc24
NetworkManager-pptp-1.2.0-1.fc24

190591 - Fedora Linux 22 FEDORA-2016-6fd7a31d36 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4021

Description

The scan detected that the host is missing the following update:
FEDORA-2016-6fd7a31d36

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184617.html

Fedora Core 22

pgpdump-0.30-1.fc22

190593 - Fedora Linux 24 FEDORA-2016-cc5a0a516b 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-cc5a0a516b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183613.html

Fedora Core 24

libreoffice-5.1.3.1-2.fc24

190594 - Fedora Linux 24 FEDORA-2016-92e9f47c04 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-2016-92e9f47c04

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184045.html

Fedora Core 24

thunderbird-45.0-2.fc24

190595 - Fedora Linux 24 FEDORA-2016-bf916bcc04 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4414

Description

The scan detected that the host is missing the following update:
FEDORA-2016-bf916bcc04

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183746.html

Fedora Core 24

quassel-0.12.4-1.fc24

190596 - Fedora Linux 24 FEDORA-2016-b732d126f9 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-b732d126f9

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183602.html

Fedora Core 24

firefox-46.0.1-1.fc24

190598 - Fedora Linux 24 FEDORA-2016-aff691237e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2181, CVE-2015-8864, CVE-2016-4068, CVE-2016-4069

Description

The scan detected that the host is missing the following update:
FEDORA-2016-aff691237e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184089.html

Fedora Core 24

roundcubemail-1.1.5-1.fc24

190599 - Fedora Linux 23 FEDORA-2016-42f30d76a0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4414

Description

The scan detected that the host is missing the following update:
FEDORA-2016-42f30d76a0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183571.html

Fedora Core 23

quassel-0.12.4-1.fc23

190600 - Fedora Linux 24 FEDORA-2016-a545f81683 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7827, CVE-2016-2849, CVE-2016-2850

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a545f81683

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183669.html

Fedora Core 24

botan-1.10.13-1.fc24

190601 - Fedora Linux 24 FEDORA-2016-679c4ddd3c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3096

Description

The scan detected that the host is missing the following update:
FEDORA-2016-679c4ddd3c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184175.html

Fedora Core 24

ansible-2.0.2.0-1.fc24

190602 - Fedora Linux 22 FEDORA-2016-c1bad2b755 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-c1bad2b755

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184620.html

Fedora Core 22

thunderbird-45.0-2.fc22

190603 - Fedora Linux 24 FEDORA-2016-94f8ac45bb 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-2016-94f8ac45bb

Observation

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

For more information see:

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184213.html

Fedora Core 24

i7z-0.27.2-16.20150629gitec09c4f.fc24

190606 - Fedora Linux 24 FEDORA-2016-cdb5052362 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-cdb5052362

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184398.html

Fedora Core 24

python-tgcaptcha2-0.3.1-1.fc24

190607 - Fedora Linux 24 FEDORA-2016-af4989be51 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-af4989be51

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183896.html

Fedora Core 24

rpm-4.13.0-0.rc1.27.fc24

190609 - Fedora Linux 22 FEDORA-2016-0431acaa78 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4414

Description

The scan detected that the host is missing the following update:
FEDORA-2016-0431acaa78

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183585.html

Fedora Core 22

quassel-0.12.4-1.fc22

190610 - Fedora Linux 24 FEDORA-2016-981aacd835 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-2016-981aacd835

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184152.html

Fedora Core 24

tmux-2.2-1.fc24

190611 - Fedora Linux 22 FEDORA-2016-e2acbd739f 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-e2acbd739f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184399.html

Fedora Core 22

firefox-46.0.1-1.fc22

190613 - Fedora Linux 24 FEDORA-2016-f4e73663f4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544

Description

The scan detected that the host is missing the following update:
FEDORA-2016-f4e73663f4

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183736.html

Fedora Core 24

php-5.6.21-1.fc24

190616 - Fedora Linux 23 FEDORA-2016-25843fda6b 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-2016-25843fda6b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183499.html

Fedora Core 23

firefox-46.0.1-1.fc23

190618 - Fedora Linux 24 FEDORA-2016-5e897e9b85 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-2016-5e897e9b85

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183722.html

Fedora Core 24

glib-networking-2.48.1-1.fc24

190619 - Fedora Linux 24 FEDORA-2016-1eaaf1ed0f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3099

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1eaaf1ed0f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184345.html

Fedora Core 24

mod_nss-1.0.12-4.fc24

190622 - Fedora Linux 24 FEDORA-2016-6c03d31846 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-2016-6c03d31846

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184392.html

Fedora Core 24

parallel-20160222-1.fc24

190623 - Fedora Linux 24 FEDORA-2016-1c4e616564 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8869

Description

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

FEDORA-2016-1c4e616564

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184507.html

Fedora Core 24

ocaml-4.02.3-3.fc24

190624 - Fedora Linux 24 FEDORA-2016-ed8c6c0426 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1548, CVE-2016-1550, CVE-2016-2516, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ed8c6c0426

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183647.html

Fedora Core 24

ntp-4.2.6p5-40.fc24

190625 - Fedora Linux 24 FEDORA-2016-8f4b54b005 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4021

Description

The scan detected that the host is missing the following update:
FEDORA-2016-8f4b54b005

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183750.html

Fedora Core 24

pgpdump-0.30-1.fc24

190627 - Fedora Linux 22 FEDORA-2016-5a9313e4b4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8853

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5a9313e4b4

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183592.html

Fedora Core 22

perl-5.20.3-330.fc22

190628 - Fedora Linux 23 FEDORA-2016-34f9ed9753 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-2016-34f9ed9753

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183501.html

Fedora Core 23

libreoffice-5.0.6.2-3.fc23

190630 - Fedora Linux 24 FEDORA-2016-4ce97823af Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4482

Description

The scan detected that the host is missing the following update:
FEDORA-2016-4ce97823af

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184414.html

Fedora Core 24

kernel-4.5.3-300.fc24

190631 - Fedora Linux 23 FEDORA-2016-5733ad20f5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4021

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5733ad20f5

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184689.html

Fedora Core 23

pgpdump-0.30-1.fc23

190632 - Fedora Linux 23 FEDORA-2016-5b2eb0bf9c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1548, CVE-2016-1550, CVE-2016-2516, CVE-2016-2518

Description

The scan detected that the host is missing the following update:
FEDORA-2016-5b2eb0bf9c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184669.html

Fedora Core 23

ntp-4.2.6p5-40.fc23

144587 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1247-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1247-1

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-May/002043.html

SuSE SLED 12
x86_64
ntp-debugsource-4.2.8p6-46.5.2
ntp-debuginfo-4.2.8p6-46.5.2
ntp-doc-4.2.8p6-46.5.2
ntp-4.2.8p6-46.5.2

noarch
yast2-ntp-client-3.1.12.4-8.2

SuSE SLES 12
noarch
yast2-ntp-client-3.1.12.4-8.2

x86_64
ntp-debugsource-4.2.8p6-46.5.2
ntp-debuginfo-4.2.8p6-46.5.2
ntp-doc-4.2.8p6-46.5.2
ntp-4.2.8p6-46.5.2

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.

12188 - HP 3COM/H3C Intelligent Management Center Img Recv Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-2331

Update Details

Recommendation is updated

908 - Microsoft IIS 4.0 /IISADMPWD/achg.htr Proxied Password Attack

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

Risk Level: High

CVE: CVE-1999-0407

Update Details

Recommendation is updated

10088 - GuildFTPd LIST and CWD Commands Heap Overflow Vulnerability

Category: General Vulnerability Assessment -> Instrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2008-4572

Update Details

Recommendation is updated

13790 - Microsoft IIS 7.5 Classic ASP Authentication Bypass Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13791 - Microsoft IIS 6.0 PHP Authentication Bypass Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13792 - Microsoft IIS 7.5 .NET Authentication Bypass Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

17621 - Hewlett Packard Vertica Monitor Thread Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

20006 - (MS16-061) Security Update for Microsoft RPC (3155520)

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

Risk Level: High

CVE: CVE-2016-0178

Update Details

Risk is updated

20008 - (MS16-061) Microsoft Windows Remote Procedure Call NDR Engine Privilege Escalation (3155520)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0178

Update Details

Risk is updated

20012 - (MS16-051) Microsoft Internet Explorer Security Bypass (3155533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0188

Update Details

Risk is updated

20019 - (MS16-055) Microsoft Windows Graphics Remote Code Execution (3156754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0170

Update Details

Risk is updated

20020 - (MS16-055) Microsoft Windows Graphics Direct3D Remote Code Execution (3156754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0184

Update Details

Risk is updated

20021 - (MS16-055) Microsoft Windows Graphics Imaging Component Remote Code Execution (3156754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0195

Update Details

Risk is updated

20030 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution I (3155544)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0126

Update Details

Risk is updated

20031 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution II (3155544)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0140

Update Details

Risk is updated

20035 - (MS16-059) Microsoft Windows Media Center Mcl file Privilege Escalation (3150220)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0185

Update Details

Risk is updated

20046 - (MS16-054) Security Update for Microsoft Office (3155544)

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

Risk Level: High

CVE: CVE-2016-0126, CVE-2016-0140, CVE-2016-0183, CVE-2016-0198

Update Details

Risk is updated

20047 - (MS16-059) Security Update for Windows Media Center (3150220)

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

Risk Level: High

CVE: CVE-2016-0185

Update Details

Risk is updated

20051 - (MS16-056) Microsoft Windows Journal Memory Corruption Remote Code Execution (3156761)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0182

Update Details

Risk is updated

20056 - (MS16-057) Microsoft Windows Shell Remote Code Execution (3156987)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0179

Update Details

Risk is updated

20070 - (MS16-054) Security Update for Microsoft Office (3155544)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0126, CVE-2016-0140, CVE-2016-0183, CVE-2016-0198

Update Details

Risk is updated

875 - Microsoft IIS Anonymous Write Permissions Enabled

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

14806 - HMS Netbiter Config Utility Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

8198 - Microsoft IIS ASP.NET Cookie Header Information Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12929 - HP Data Protector Media Operations Directory Traversal Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

12930 - HP Data Protector Media Operations Heap Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

16205 - HP 2620 Switches /html/json.html Admin Account Manipulation Cross-Site Request Forgery

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: High

CVE: CVE-2013-6852

Update Details

Recommendation is updated

20007 - (MS16-058) Security Update for Windows IIS (3141083)

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

Risk Level: High

CVE: CVE-2016-0152

Update Details

Risk is updated

20011 - (MS16-051) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution I (3155533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0187

Update Details

Risk is updated

20013 - (MS16-051) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3155533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0189

Update Details

Risk is updated

20014 - (MS16-051) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution (3155533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0192

Update Details

Risk is updated

20026 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3155538)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0186

Update Details

Risk is updated

20027 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3155538)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0191

Update Details

Risk is updated

20028 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3155538)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0193

Update Details

Risk is updated

20029 - (MS16-052) Microsoft Edge Memory Corruption Remote Code Execution (3155538)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0192

Update Details

Risk is updated

20036 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation I (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0176

Update Details

Risk is updated

20038 - (MS16-062) Microsoft Windows Kernel Privilege Escalation IV (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0174

Update Details

Risk is updated

20039 - (MS16-062) Microsoft Windows Kernel Privilege Escalation III (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0173

Update Details

Risk is updated

20041 - (MS16-062) Microsoft Windows Kernel Privilege Escalation I (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0171

Update Details

Risk is updated

20042 - (MS16-062) Security Update for Windows Kernel-Mode Drivers (3158222)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0171, CVE-2016-0173, CVE-2016-0174, CVE-2016-0175, CVE-2016-0176, CVE-2016-0196, CVE-2016-0197

Update Details

Risk is updated

20043 - (MS16-060) Microsoft Windows Kernel Symbolic Links Privilege Escalation (3154846)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0180

Update Details

Risk is updated

20045 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation II (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0197

Update Details

Risk is updated

20048 - (MS16-060) Security Update for Windows Kernel (3154846)

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

Risk Level: High

CVE: CVE-2016-0180

Update Details

Risk is updated

20050 - (MS16-062) Microsoft Windows Kernel Privilege Escalation V (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0196

Update Details

Risk is updated

20053 - (MS16-053) Microsoft VBScript Memory Corruption Remote Code Execution II (3156764)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0189

Update Details

Risk is updated

20054 - (MS16-053) Microsoft VBScript Memory Corruption Remote Code Execution I (3156764)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0187

Update Details

Risk is updated

20055 - (MS16-053) Security Update for JScript and VBScript (3156764)

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

Risk Level: High

CVE: CVE-2016-0187, CVE-2016-0189

Update Details

Risk is updated

20064 - (MS16-052) Cumulative Security Update for Microsoft Edge (3155538)

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

Risk Level: High

CVE: CVE-2016-0186, CVE-2016-0191, CVE-2016-0192, CVE-2016-0193

Update Details

Risk is updated

3052 - Grokster FastTrack P2P Supernode Packet Handler Buffer Overrun

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

Risk Level: Medium

CVE: CVE-2003-0397

Update Details

Recommendation is updated

181937 - FreeBSD mercurial Arbitrary Code Execution Vulnerability (78abc022-0fee-11e6-9a1c-0014a5a57822)

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

Risk Level: Medium

CVE: CVE-2016-3105

Update Details

Risk is updated

13968 - Honeywell PowerNet Twin Client RFSync.exe Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

3861 - Home FTP Information Disclosure

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

Risk Level: Medium

CVE: CVE-2005-2726, CVE-2005-2727, CVE-2006-0355, CVE-2006-0356

Update Details

Recommendation is updated

20017 - (MS16-055) Microsoft Windows Graphics Information Disclosure I (3156754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0168

Update Details

Risk is updated

20018 - (MS16-055) Microsoft Windows Graphics Information Disclosure II (3156754)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0169

Update Details

Risk is updated

130485 - Debian Linux 8.0 DSA-3568-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4008

Update Details

Risk is updated

181925 - FreeBSD libtasn1 Denial Of Service Parsing Malicious DER Certificates (1b0d2938-0766-11e6-94fa-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details
Risk is updated

185251 - Ubuntu Linux 16.04 USN-2957-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details
Risk is updated

185254 - Ubuntu Linux 12.04, 14.04, 15.10 USN-2957-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details
Risk is updated

190522 - Fedora Linux 24 FEDORA-2016-048ffb6235 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details
Risk is updated

190555 - Fedora Linux 23 FEDORA-2016-383b8250e6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details
Risk is updated

190578 - Fedora Linux 22 FEDORA-2016-96bfd9e873 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4008

Update Details

Risk is updated

821 - Microsoft IIS 4.0 bdir.htr Directory Disclosure

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

825 - Microsoft IIS 4.0 Unicode ASP Source Disclosure

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

Risk Level: Low

CVE: CVE-2001-0709

Update Details

Recommendation is updated

10065 - Home FTP Server 'MKD' Command Multiple Directory Traversal Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Low

CVE: CVE-2009-4053

Update Details

Recommendation is updated

883 - Microsoft IIS Blank Host Auth Internal IP Disclosure

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

Risk Level: Low

CVE: CVE-2002-0422

Update Details

Recommendation is updated

20015 - (MS16-051) Microsoft Internet Explorer Information Disclosure (3155533)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0194

Update Details

Risk is updated

20024 - (MS16-066) Microsoft Windows Hypervisor Code Integrity Security Bypass (3155451)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0181

Update Details

Risk is updated

20025 - (MS16-066) Security Update for Virtual Secure Mode (3155451)

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

Risk Level: Low

CVE: CVE-2016-0181

Update Details

Risk is updated

20034 - (MS16-067) Security Update for Volume Manager Driver (3155784)

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

Risk Level: Low

CVE: CVE-2016-0190

Update Details

Risk is updated

20037 - (MS16-062) Microsoft Windows Kernel Information Disclosure (3158222)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0175

Update Details

Risk is updated

20044 - (MS16-067) Microsoft Windows USB Driver RDP Drive Redirection Information Disclosure (3155784)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0190

Update Details

Risk is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly

urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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

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

Copyright 2016 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates