2015-DEC-17
FSL version 7.5.775

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

19437 - (HT205642) Apple Xcode Multiple Vulnerabilities Prior To 7.2

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

Risk Level: High

CVE: CVE-2015-7049, CVE-2015-7056, CVE-2015-7057, CVE-2015-7082

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, IDE SCM and otools components. Successful exploitation could allow an attacker to cause a denial of service condition, to retrieve sensitive information, to escalate privileges or to remotely execute arbitrary code.

19438 - IBM AIX Java Multiple Vulnerabilities (October 2015 CPU)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4810, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4871, CVE-2015-4872, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4902, CVE-2015-4903, CVE-2015-4911, CVE-2015-5006

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 SDK. Successful exploitation could allow an attacker to completely affect integrity, availability and confidentiality of the target system.

19439 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.80

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

Risk Level: High

CVE: CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791, CVE-2015-8548

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 arbitrary code or cause a denial of service condition.

19440 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.80

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791, CVE-2015-8548

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 arbitrary code or cause a denial of service condition.

130333 - Debian Linux 8.0 DSA-3415-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1302, CVE-2015-6764, CVE-2015-6765, CVE-2015-6766, CVE-2015-6767, CVE-2015-6768, CVE-2015-6769, CVE-2015-6770, CVE-2015-6771, CVE-2015-6772, CVE-2015-6773, CVE-2015-6774, CVE-2015-6775, CVE-2015-6776, CVE-2015-6777, CVE-2015-6778, CVE-2015-6779, CVE-2015-6780, CVE-2015-6781, CVE-2015-6782, CVE-2015-6784, CVE-2015-6785, CVE-2015-6786

Description

The scan detected that the host is missing the following update:
DSA-3415-1

Observation

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

http://www.debian.org/security/2015/dsa-3415

Debian 8.0
all
chromium-l10n_47.0.2526.73-1~deb8u1
chromium-inspector_47.0.2526.73-1~deb8u1
chromium-dbg_47.0.2526.73-1~deb8u1
chromedriver_47.0.2526.73-1~deb8u1
chromium_47.0.2526.73-1~deb8u1

130338 - Debian Linux 8.0 DSA-3418-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791

Description

The scan detected that the host is missing the following update:
DSA-3418-1

Observation

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

http://www.debian.org/security/2015/dsa-3418

Debian 8.0
all
chromium-l10n_47.0.2526.80-1~deb8u1
chromium-dbg_47.0.2526.80-1~deb8u1
chromedriver_47.0.2526.80-1~deb8u1
chromium-inspector_47.0.2526.80-1~deb8u1
chromium_47.0.2526.80-1~deb8u1

141034 - Red Hat Enterprise Linux RHSA-2015-2618 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791, CVE-2015-8548

Description

The scan detected that the host is missing the following update:
RHSA-2015-2618

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2618.html

RHEL6D
x86_64
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

i386
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

RHEL6S
x86_64
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

i386
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

RHEL6WS
x86_64
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

i386
chromium-browser-debuginfo-47.0.2526.80-1.el6
chromium-browser-47.0.2526.80-1.el6

141035 - Red Hat Enterprise Linux RHSA-2015-2593 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8454, CVE-2015-8455, CVE-2015-8456, CVE-2015-8457

Description

The scan detected that the host is missing the following update:
RHSA-2015-2593

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2593.html

RHEL5S
x86_64
flash-plugin-11.2.202.554-1.el5

i386
flash-plugin-11.2.202.554-1.el5

RHEL6D
x86_64
flash-plugin-11.2.202.554-1.el6_7

i386
flash-plugin-11.2.202.554-1.el6_7

RHEL6S
x86_64
flash-plugin-11.2.202.554-1.el6_7

i386
flash-plugin-11.2.202.554-1.el6_7

RHEL6WS
x86_64
flash-plugin-11.2.202.554-1.el6_7

i386
flash-plugin-11.2.202.554-1.el6_7

RHEL5D
x86_64
flash-plugin-11.2.202.554-1.el5

i386
flash-plugin-11.2.202.554-1.el5

144086 - SuSE SLED 12 SUSE-SU-2015:2247-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8454, CVE-2015-8455

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2247-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-December/001729.html

SuSE SLED 12
x86_64
flash-player-gnome-11.2.202.554-114.1
flash-player-11.2.202.554-114.1

170604 - Amazon Linux AMI ALAS-2015-616 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
ALAS-2015-616

Observation

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

https://alas.aws.amazon.com/ALAS-2015-616.html

Amazon Linux AMI
x86_64
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.72.amzn1

i686
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.72.amzn1
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.72.amzn1

174717 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-9353)

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

Risk Level: High

CVE: CVE-2015-2724, CVE-2015-2725, CVE-2015-2731, CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740, CVE-2015-2741

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-9353)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=9353

SL5
x86_64
thunderbird-31.8.0-1.el5_11
thunderbird-debuginfo-31.8.0-1.el5_11

i386
thunderbird-31.8.0-1.el5_11
thunderbird-debuginfo-31.8.0-1.el5_11

SL7
x86_64
thunderbird-31.8.0-1.el7_1
thunderbird-debuginfo-31.8.0-1.el7_1

SL6
x86_64
thunderbird-31.8.0-1.el6_6
thunderbird-debuginfo-31.8.0-1.el6_6

i386
thunderbird-31.8.0-1.el6_6
thunderbird-debuginfo-31.8.0-1.el6_6

174718 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-14290)

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

Risk Level: High

CVE: CVE-2015-4473, CVE-2015-4475, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4484, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4491, CVE-2015-4492, CVE-2015-4493

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-14290)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=14290

SL5
x86_64
firefox-38.2.0-4.el5_11
firefox-debuginfo-38.2.0-4.el5_11

i386
firefox-38.2.0-4.el5_11
firefox-debuginfo-38.2.0-4.el5_11

SL7
x86_64
firefox-38.2.0-4.el7_1
firefox-debuginfo-38.2.0-4.el7_1

SL6
x86_64
firefox-debuginfo-38.2.0-4.el6_7
firefox-38.2.0-4.el6_7

i386
firefox-debuginfo-38.2.0-4.el6_7
firefox-38.2.0-4.el6_7

174723 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1510-2612)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1510-2612)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=2612

SL5
x86_64
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.1.el5_11

i386
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.1.el5_11
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.1.el5_11

174739 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1507-6856)

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

Risk Level: High

CVE: CVE-2015-2590, CVE-2015-2601, CVE-2015-2621, CVE-2015-2625, CVE-2015-2628, CVE-2015-2632, CVE-2015-2808, CVE-2015-4000, CVE-2015-4731, CVE-2015-4732, CVE-2015-4733, CVE-2015-4748, CVE-2015-4749, CVE-2015-4760

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.7.0-openjdk on SL5.x i386/x86_64 (1507-6856)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=6856

SL5
x86_64
java-1.7.0-openjdk-devel-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-src-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-demo-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.85-2.6.1.3.el5_11

i386
java-1.7.0-openjdk-devel-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-src-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-demo-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-debuginfo-1.7.0.85-2.6.1.3.el5_11
java-1.7.0-openjdk-javadoc-1.7.0.85-2.6.1.3.el5_11

174740 - Scientific Linux Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-14793)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-14793)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=14793

SL5
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el5_11
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el5_11

SL7
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el7_1
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el7_1

SL6
x86_64
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

i386
java-1.6.0-openjdk-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-src-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-javadoc-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-devel-1.6.0.37-1.13.9.4.el6_7
java-1.6.0-openjdk-demo-1.6.0.37-1.13.9.4.el6_7

174755 - Scientific Linux Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1510-3884)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1510-3884)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=3884

SL7
x86_64
java-1.7.0-openjdk-headless-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.1.el7_1
java-1.7.0-openjdk-accessibility-1.7.0.91-2.6.2.1.el7_1

noarch
java-1.7.0-openjdk-javadoc-1.7.0.91-2.6.2.1.el7_1

SL6
i386
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.2.el6_7

noarch
java-1.7.0-openjdk-javadoc-1.7.0.91-2.6.2.2.el6_7

x86_64
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.2.el6_7
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.2.el6_7

174774 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-24093)

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

Risk Level: High

CVE: CVE-2015-4473, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4491

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-24093)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=24093

SL5
x86_64
thunderbird-debuginfo-38.2.0-4.el5_11
thunderbird-38.2.0-4.el5_11

i386
thunderbird-debuginfo-38.2.0-4.el5_11
thunderbird-38.2.0-4.el5_11

SL7
x86_64
thunderbird-debuginfo-38.2.0-1.el7_1
thunderbird-38.2.0-1.el7_1

SL6
x86_64
thunderbird-38.2.0-4.el6_7
thunderbird-debuginfo-38.2.0-4.el6_7

i386
thunderbird-38.2.0-4.el6_7
thunderbird-debuginfo-38.2.0-4.el6_7

174782 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-75)

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

Risk Level: High

CVE: CVE-2015-2722, CVE-2015-2724, CVE-2015-2725, CVE-2015-2727, CVE-2015-2728, CVE-2015-2729, CVE-2015-2731, CVE-2015-2733, CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740, CVE-2015-2741, CVE-2015-2743

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-75)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=75

SL5
x86_64
firefox-38.1.0-1.el5_11
firefox-debuginfo-38.1.0-1.el5_11

i386
firefox-38.1.0-1.el5_11
firefox-debuginfo-38.1.0-1.el5_11

SL7
x86_64

firefox-38.1.0-1.el7_1
firefox-debuginfo-38.1.0-1.el7_1

SL6
x86_64
firefox-debuginfo-38.1.0-1.el6_6
firefox-38.1.0-1.el6_6

i386
firefox-debuginfo-38.1.0-1.el6_6
firefox-38.1.0-1.el6_6

174786 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1507-8420)

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

Risk Level: High

CVE: CVE-2015-0383, CVE-2015-2590, CVE-2015-2601, CVE-2015-2621, CVE-2015-2625, CVE-2015-2628, CVE-2015-2632, CVE-2015-2659, CVE-2015-2808, CVE-2015-3149, CVE-2015-4000, CVE-2015-4731, CVE-2015-4732, CVE-2015-4733, CVE-2015-4748, CVE-2015-4749, CVE-2015-4760

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1507-8420)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=8420

SL7
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-src-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-headless-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-demo-1.8.0.51-1.b16.el7_1
java-1.8.0-openjdk-devel-1.8.0.51-1.b16.el7_1

noarch
java-1.8.0-openjdk-javadoc-1.8.0.51-1.b16.el7_1

SL6
i386
java-1.8.0-openjdk-devel-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-headless-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-demo-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-debuginfo-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-src-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-1.8.0.51-0.b16.el6_6

noarch
java-1.8.0-openjdk-javadoc-1.8.0.51-0.b16.el6_6

x86_64
java-1.8.0-openjdk-devel-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-headless-1.8.0.51-0.b16.el6_6

java-1.8.0-openjdk-demo-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-debuginfo-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-src-1.8.0.51-0.b16.el6_6
java-1.8.0-openjdk-1.8.0.51-0.b16.el6_6

174798 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1510-3234)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4868, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4903, CVE-2015-4911

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1510-3234)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=3234

SL7
x86_64
java-1.8.0-openjdk-accessibility-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-debuginfo-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-demo-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-src-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-headless-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-devel-1.8.0.65-2.b17.el7_1
java-1.8.0-openjdk-1.8.0.65-2.b17.el7_1

noarch
java-1.8.0-openjdk-javadoc-1.8.0.65-2.b17.el7_1

SL6
i386
java-1.8.0-openjdk-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-debuginfo-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-headless-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-devel-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-devel-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-demo-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-src-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.65-0.b17.el6_7

noarch
java-1.8.0-openjdk-javadoc-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-javadoc-1.8.0.65-0.b17.el6_7

x86_64
java-1.8.0-openjdk-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-debuginfo-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-headless-1.8.0.65-0.b17.el6_7

java-1.8.0-openjdk-devel-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-demo-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-devel-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-demo-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-src-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-src-debug-1.8.0.65-0.b17.el6_7
java-1.8.0-openjdk-headless-debug-1.8.0.65-0.b17.el6_7

174807 - Scientific Linux Security ERRATA Important: cups on SL6.x, SL7.x i386/x86_64 (1506-11940)

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

Risk Level: High

CVE: CVE-2014-9679, CVE-2015-1158, CVE-2015-1159

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: cups on SL6.x, SL7.x i386/x86_64 (1506-11940)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=11940

SL7
x86_64
cups-1.6.3-17.el7_1.1
cups-devel-1.6.3-17.el7_1.1
cups-libs-1.6.3-17.el7_1.1
cups-client-1.6.3-17.el7_1.1
cups-lpd-1.6.3-17.el7_1.1
cups-ipptool-1.6.3-17.el7_1.1
cups-debuginfo-1.6.3-17.el7_1.1

noarch
cups-filesystem-1.6.3-17.el7_1.1

SL6
x86_64
cups-1.4.2-67.el6_6.1
cups-devel-1.4.2-67.el6_6.1
cups-debuginfo-1.4.2-67.el6_6.1
cups-php-1.4.2-67.el6_6.1
cups-libs-1.4.2-67.el6_6.1
cups-lpd-1.4.2-67.el6_6.1

i386
cups-1.4.2-67.el6_6.1
cups-devel-1.4.2-67.el6_6.1
cups-debuginfo-1.4.2-67.el6_6.1
cups-php-1.4.2-67.el6_6.1
cups-libs-1.4.2-67.el6_6.1
cups-lpd-1.4.2-67.el6_6.1

174818 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-24515)

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

Risk Level: High

CVE: CVE-2015-4497, CVE-2015-4498

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-24515)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=24515

SL5
x86_64
firefox-38.2.1-1.el5_11
firefox-debuginfo-38.2.1-1.el5_11

i386
firefox-38.2.1-1.el5_11
firefox-debuginfo-38.2.1-1.el5_11

SL7
x86_64
firefox-38.2.1-1.el7_1
firefox-debuginfo-38.2.1-1.el7_1

SL6
x86_64
firefox-debuginfo-38.2.1-1.el6_7
firefox-38.2.1-1.el6_7

i386
firefox-debuginfo-38.2.1-1.el6_7
firefox-38.2.1-1.el6_7

174819 - Scientific Linux Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1507-7844)

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

Risk Level: High

CVE: CVE-2015-2590, CVE-2015-2601, CVE-2015-2621, CVE-2015-2625, CVE-2015-2628, CVE-2015-2632, CVE-2015-2808, CVE-2015-4000, CVE-2015-4731, CVE-2015-4732, CVE-2015-4733, CVE-2015-4748, CVE-2015-4749, CVE-2015-4760

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86_64 (1507-7844)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=7844

SL7
x86_64
java-1.7.0-openjdk-accessibility-1.7.0.85-2.6.1.2.el7_1

java-1.7.0-openjdk-debuginfo-1.7.0.85-2.6.1.2.el7_1
java-1.7.0-openjdk-src-1.7.0.85-2.6.1.2.el7_1
java-1.7.0-openjdk-devel-1.7.0.85-2.6.1.2.el7_1
java-1.7.0-openjdk-headless-1.7.0.85-2.6.1.2.el7_1
java-1.7.0-openjdk-1.7.0.85-2.6.1.2.el7_1
java-1.7.0-openjdk-demo-1.7.0.85-2.6.1.2.el7_1

noarch
java-1.7.0-openjdk-javadoc-1.7.0.85-2.6.1.2.el7_1

SL6
i386
java-1.7.0-openjdk-demo-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-src-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-devel-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-debuginfo-1.7.0.85-2.6.1.3.el6_6

noarch
java-1.7.0-openjdk-javadoc-1.7.0.85-2.6.1.3.el6_6

x86_64
java-1.7.0-openjdk-demo-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-src-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-devel-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-1.7.0.85-2.6.1.3.el6_6
java-1.7.0-openjdk-debuginfo-1.7.0.85-2.6.1.3.el6_6

174826 - Scientific Linux Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-8436)

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

Risk Level: High

CVE: CVE-2015-2590, CVE-2015-2601, CVE-2015-2621, CVE-2015-2625, CVE-2015-2628, CVE-2015-2632, CVE-2015-2808, CVE-2015-4000, CVE-2015-4731, CVE-2015-4732, CVE-2015-4733, CVE-2015-4748, CVE-2015-4749, CVE-2015-4760

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-8436)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=8436

SL5
x86_64
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-demo-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-javadoc-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-src-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.36-1.13.8.1.el5_11

i386
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-devel-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-demo-1.6.0.36-1.13.8.1.el5_11

java-1.6.0-openjdk-javadoc-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-src-1.6.0.36-1.13.8.1.el5_11
java-1.6.0-openjdk-debuginfo-1.6.0.36-1.13.8.1.el5_11

SL7
x86_64
java-1.6.0-openjdk-src-1.6.0.36-1.13.8.1.el7_1
java-1.6.0-openjdk-demo-1.6.0.36-1.13.8.1.el7_1
java-1.6.0-openjdk-javadoc-1.6.0.36-1.13.8.1.el7_1
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el7_1
java-1.6.0-openjdk-devel-1.6.0.36-1.13.8.1.el7_1
java-1.6.0-openjdk-debuginfo-1.6.0.36-1.13.8.1.el7_1

SL6
x86_64
java-1.6.0-openjdk-javadoc-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-src-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-demo-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-devel-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el6_7

i386
java-1.6.0-openjdk-javadoc-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-src-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-demo-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-devel-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-debuginfo-1.6.0.36-1.13.8.1.el6_7
java-1.6.0-openjdk-1.6.0.36-1.13.8.1.el6_7

178072 - Gentoo Linux GLSA-201503-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0332, CVE-2015-0333, CVE-2015-0334, CVE-2015-0335, CVE-2015-0336, CVE-2015-0337, CVE-2015-0338, CVE-2015-0339, CVE-2015-0340, CVE-2015-0341, CVE-2015-0342

Description

The scan detected that the host is missing the following update:
GLSA-201503-09

Observation

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

https://security.gentoo.org/glsa/201503-09

Affected packages:
www-plugins/adobe-flash < 11.2.202.451

178082 - Gentoo Linux GLSA-201506-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3096, CVE-2015-3097, CVE-2015-3098, CVE-2015-3099, CVE-2015-3100, CVE-2015-3101, CVE-2015-3102, CVE-2015-3103, CVE-2015-3104, CVE-2015-3105, CVE-2015-3106, CVE-2015-3107, CVE-2015-3108, CVE-2015-4472

Description

The scan detected that the host is missing the following update:
GLSA-201506-01

Observation

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

https://security.gentoo.org/glsa/201506-01

Affected packages:
www-plugins/adobe-flash < 11.2.202.466

178086 - Gentoo Linux GLSA-201507-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0578, CVE-2015-3113, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116, CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432, CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118, CVE-2015-5119

Description

The scan detected that the host is missing the following update:
GLSA-201507-13

Observation

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

https://security.gentoo.org/glsa/201507-13

Affected packages:
www-plugins/adobe-flash < 11.2.202.481

178091 - Gentoo Linux GLSA-201509-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2806, CVE-2015-3622

Description

The scan detected that the host is missing the following update:
GLSA-201509-04

Observation

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

https://security.gentoo.org/glsa/201509-04

Affected packages:
dev-libs/libtasn1 < 1.4.5

178092 - Gentoo Linux GLSA-201509-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5567, CVE-2015-5568, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6679, CVE-2015-6680, CVE-2015-6681, CVE-2015-6682

Description

The scan detected that the host is missing the following update:
GLSA-201509-07

Observation

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

https://security.gentoo.org/glsa/201509-07

Affected packages:
www-plugins/adobe-flash < 11.2.202.521

178094 - Gentoo Linux GLSA-201508-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3107, CVE-2015-5122, CVE-2015-5123, CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5564, CVE-2015-5965

Description

The scan detected that the host is missing the following update:
GLSA-201508-01

Observation

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

https://security.gentoo.org/glsa/201508-01

Affected packages:
www-plugins/adobe-flash < 11.2.202.508

178103 - Gentoo Linux GLSA-201510-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1158, CVE-2015-1159

Description

The scan detected that the host is missing the following update:
GLSA-201510-07

Observation

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

https://security.gentoo.org/glsa/201510-07

Affected packages:
net-print/cups < 2.0.3

178119 - Gentoo Linux GLSA-201511-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5569, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628, CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE-2015-7634, CVE-2015-7643, CVE-2015-7644, CVE-2015-7645, CVE-2015-7646, CVE-2015-7647, CVE-2015-7648, CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7659, CVE-2015-7660, CVE-2015-7661, CVE-2015-7662, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, CVE-2015-8046

Description

The scan detected that the host is missing the following update:
GLSA-201511-02

Observation

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

https://security.gentoo.org/glsa/201511-02

Affected packages:
www-plugins/adobe-flash < 11.2.202.548

178122 - Gentoo Linux GLSA-201504-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0346, CVE-2015-0347, CVE-2015-0348, CVE-2015-0349, CVE-2015-0350, CVE-2015-0351, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0356, CVE-2015-0357, CVE-2015-0358, CVE-2015-0359, CVE-2015-0360, CVE-2015-3038, CVE-2015-3039, CVE-2015-3040, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043, CVE-2015-3044

Description

The scan detected that the host is missing the following update:
GLSA-201504-07

Observation

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

https://security.gentoo.org/glsa/201504-07

Affected packages:
www-plugins/adobe-flash < 11.2.202.457

178123 - Gentoo Linux GLSA-201505-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3044, CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081, CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-2015-3092, CVE-2015-3093

Description

The scan detected that the host is missing the following update:
GLSA-201505-02

Observation

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

https://security.gentoo.org/glsa/201505-02

Affected packages:
www-plugins/adobe-flash < 11.2.202.460

178127 - Gentoo Linux GLSA-201504-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-2566, CVE-2013-5593, CVE-2013-5595, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602, CVE-2013-5603, CVE-2013-5604, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607, CVE-2013-5609, CVE-2013-5610, CVE-2013-5612, CVE-2013-5613, CVE-2013-5614, CVE-2013-5615, CVE-2013-5616, CVE-2013-5618, CVE-2013-5619, CVE-2013-6671, CVE-2013-6672, CVE-2013-6673, CVE-2014-1477, CVE-2014-1480, CVE-2014-1482, CVE-2014-1483, CVE-2014-1485, CVE-2014-1486, CVE-2014-1487, CVE-2014-1488, CVE-2014-1490, CVE-2014-1492, CVE-2014-1493, CVE-2014-1494, CVE-2014-1497, CVE-2014-1498, CVE-2014-1500, CVE-2014-1502, CVE-2014-1504, CVE-2014-1505, CVE-2014-1508, CVE-2014-1509, CVE-2014-1510, CVE-2014-1511, CVE-2014-1512, CVE-2014-1513, CVE-2014-1514, CVE-2014-1518, CVE-2014-1519, CVE-2014-1520, CVE-2014-1522, CVE-2014-1523, CVE-2014-1524, CVE-2014-1525, CVE-2014-1526, CVE-2014-1529, CVE-2014-1530, CVE-2014-1531, CVE-2014-1532, CVE-2014-1533, CVE-2014-1534, CVE-2014-1536, CVE-2014-1537, CVE-2014-1538, CVE-2014-1539, CVE-2014-1547, CVE-2014-1550, CVE-2014-1551, CVE-2014-1552, CVE-2014-1553, CVE-2014-1554, CVE-2014-1555, CVE-2014-1556, CVE-2014-1557, CVE-2014-1558, CVE-2014-1559, CVE-2014-1560, CVE-2014-1561, CVE-2014-1562, CVE-2014-1563, CVE-2014-1564, CVE-2014-1565, CVE-2014-1566, CVE-2014-1567, CVE-2014-1568, CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1580, CVE-2014-1581, CVE-2014-1582, CVE-2014-1583, CVE-2014-1584, CVE-2014-1585, CVE-2014-1586, CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-5369, CVE-2014-8631, CVE-2014-8632, CVE-2014-8634, CVE-2014-8635, CVE-2014-8636, CVE-2014-8637, CVE-2014-8638, CVE-2014-8639, CVE-2014-8640, CVE-2014-8641, CVE-2014-8642, CVE-2015-0820, CVE-2015-0821, CVE-2015-0822, CVE-2015-0823, CVE-2015-0824, CVE-2015-0825, CVE-2015-0826, CVE-2015-0827, CVE-2015-0828, CVE-2015-0829, CVE-2015-0830, CVE-2015-0831, CVE-2015-0832, CVE-2015-0833, CVE-2015-0834, CVE-2015-0835, CVE-2015-0836

Description

The scan detected that the host is missing the following update:
GLSA-201504-01

Observation

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

https://security.gentoo.org/glsa/201504-01

Affected packages:
www-client/firefox < 31.5.3
www-client/firefox-bin < 31.5.3
mail-client/thunderbird < 31.5.0

mail-client/thunderbird-bin < 31.5.0
www-client/seamonkey < 2.33.1
www-client/seamonkey-bin < 2.33.1
dev-libs/nspr < 4.10.6

178131 - Gentoo Linux GLSA-201507-14 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3566, CVE-2014-6549, CVE-2014-6585, CVE-2014-6587, CVE-2014-6591, CVE-2014-6593, CVE-2014-6601, CVE-2015-0383, CVE-2015-0395, CVE-2015-0400, CVE-2015-0403, CVE-2015-0406, CVE-2015-0407, CVE-2015-0408, CVE-2015-0410, CVE-2015-0412, CVE-2015-0413, CVE-2015-0421

Description

The scan detected that the host is missing the following update:
GLSA-201507-14

Observation

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

https://security.gentoo.org/glsa/201507-14

Affected packages:
dev-java/oracle-jre-bin < 1.8.0.31
dev-java/oracle-jre-bin < 1.7.0.76
dev-java/oracle-jdk-bin < 1.8.0.31
dev-java/oracle-jdk-bin < 1.7.0.76

181710 - FreeBSD mozilla Multiple Vulnerabilities (2c2d1c39-1396-459a-91f5-ca03ee7c64c6)

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223

Description

The scan detected that the host is missing the following update:
mozilla -- multiple vulnerabilities (2c2d1c39-1396-459a-91f5-ca03ee7c64c6)

Observation

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

http://www.vuxml.org/freebsd/2c2d1c39-1396-459a-91f5-ca03ee7c64c6.html

Affected packages:
firefox < 43.0,1
linux-firefox < 43.0,1
seamonkey < 2.40
linux-seamonkey < 2.40
firefox-esr < 38.5.0,1
libxul < 38.5.0
thunderbird < 38.5.0
linux-thunderbird < 38.5.0

181713 - FreeBSD java Multiple Vulnerabilities (a5934ba8-a376-11e5-85e9-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4810, CVE-2015-4835, CVE-2015-4840, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4868, CVE-2015-4871, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2015-4901, CVE-2015-4902, CVE-2015-4903, CVE-2015-4906, CVE-2015-4908, CVE-2015-4911, CVE-2015-4916

Description

The scan detected that the host is missing the following update:
java -- multiple vulnerabilities (a5934ba8-a376-11e5-85e9-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/a5934ba8-a376-11e5-85e9-14dae9d210b8.html

Affected packages:
openjdk8 < 8.66.17
openjdk8-jre < 8.66.17

181716 - FreeBSD chromium Multiple Vulnerabilities (72c145df-a1e0-11e5-8ad0-00262d5ed8ee)

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

Risk Level: High

CVE: CVE-2015-6788, CVE-2015-6789, CVE-2015-6790, CVE-2015-6791

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (72c145df-a1e0-11e5-8ad0-00262d5ed8ee)

Observation

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

http://www.vuxml.org/freebsd/72c145df-a1e0-11e5-8ad0-00262d5ed8ee.html

Affected packages:
chromium < 47.0.2526.80
chromium-npapi < 47.0.2526.80
chromium-pulse < 47.0.2526.80

185082 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2825-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6765, CVE-2015-6766, CVE-2015-6767, CVE-2015-6768, CVE-2015-6769, CVE-2015-6770, CVE-2015-6771, CVE-2015-6772, CVE-2015-6773, CVE-2015-6777, CVE-2015-6782, CVE-2015-6784, CVE-2015-6785, CVE-2015-6786, CVE-2015-6787, CVE-2015-8478

Description

The scan detected that the host is missing the following update:
USN-2825-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003215.html

Ubuntu 15.04

liboxideqtcore0_1.11.3-0ubuntu0.15.04.1

Ubuntu 15.10

liboxideqtcore0_1.11.3-0ubuntu0.15.10.1

Ubuntu 14.04

liboxideqtcore0_1.11.3-0ubuntu0.14.04.1

185083 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2833-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223

Description

The scan detected that the host is missing the following update:
USN-2833-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003220.html

Ubuntu 12.04

firefox_43.0+build1-0ubuntu0.12.04.1

Ubuntu 15.04

firefox_43.0+build1-0ubuntu0.15.04.1

Ubuntu 15.10

firefox_43.0+build1-0ubuntu0.15.10.1

Ubuntu 14.04

firefox_43.0+build1-0ubuntu0.14.04.1

19425 - SearchBlox File Exfiltration Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2015-7919

Description

A file exfiltration vulnerability is present in some versions of SearchBlox.

Observation

SearchBlox is an enterprise elastic search engine.

A file exfiltration vulnerability is present in some versions of SearchBlox. The flaw occurs due to improper permission validation. Successful exploitation could allow an attacker to export or overwrite the config file, causing a crash.

19435 - (HT205635) Apple iOS Multiple Vulnerabilities Prior To 9.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2011-2895, CVE-2015-3807, CVE-2015-7001, CVE-2015-7037, CVE-2015-7038, CVE-2015-7039, CVE-2015-7040, CVE-2015-7041, CVE-2015-7042, CVE-2015-7043, CVE-2015-7046, CVE-2015-7047, CVE-2015-7048, CVE-2015-7050, CVE-2015-7051, CVE-2015-7053, CVE-2015-7054, CVE-2015-7055, CVE-2015-7058, CVE-2015-7064, CVE-2015-7065, CVE-2015-7066, CVE-2015-7068, CVE-2015-7069, CVE-2015-7070, CVE-2015-7072, CVE-2015-7073, CVE-2015-7074, CVE-2015-7075, CVE-2015-7079, CVE-2015-7080, CVE-2015-7081, CVE-2015-7083, CVE-2015-7084, CVE-2015-7093, CVE-2015-7094, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, CVE-2015-7103, CVE-2015-7105, CVE-2015-7107, CVE-2015-7111, CVE-2015-7112, CVE-2015-7113

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow attackers to obtain sensitive information, cause a denial of service or execute arbitrary code.

170601 - Amazon Linux AMI ALAS-2015-631 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
ALAS-2015-631

Observation

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

https://alas.aws.amazon.com/ALAS-2015-631.html

Amazon Linux AMI
x86_64
bind-utils-9.8.2-0.30.rc1.40.amzn1
bind-chroot-9.8.2-0.30.rc1.40.amzn1

bind-debuginfo-9.8.2-0.30.rc1.40.amzn1
bind-devel-9.8.2-0.30.rc1.40.amzn1
bind-sdb-9.8.2-0.30.rc1.40.amzn1
bind-libs-9.8.2-0.30.rc1.40.amzn1
bind-9.8.2-0.30.rc1.40.amzn1

i686
bind-utils-9.8.2-0.30.rc1.40.amzn1
bind-chroot-9.8.2-0.30.rc1.40.amzn1
bind-debuginfo-9.8.2-0.30.rc1.40.amzn1
bind-devel-9.8.2-0.30.rc1.40.amzn1
bind-sdb-9.8.2-0.30.rc1.40.amzn1
bind-libs-9.8.2-0.30.rc1.40.amzn1
bind-9.8.2-0.30.rc1.40.amzn1

174814 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1506-5447)

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

Risk Level: High

CVE: CVE-2014-9419, CVE-2014-9420, CVE-2014-9585, CVE-2015-1805, CVE-2015-3331

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1506-5447)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=5447

SL6
i386
python-perf-2.6.32-504.23.4.el6
kernel-headers-2.6.32-504.23.4.el6
python-perf-debuginfo-2.6.32-504.23.4.el6
kernel-2.6.32-504.23.4.el6
kernel-debug-devel-2.6.32-504.23.4.el6
kernel-debug-debuginfo-2.6.32-504.23.4.el6
kernel-debug-2.6.32-504.23.4.el6
perf-debuginfo-2.6.32-504.23.4.el6
kernel-debuginfo-common-i686-2.6.32-504.23.4.el6
kernel-debuginfo-2.6.32-504.23.4.el6
perf-2.6.32-504.23.4.el6
kernel-devel-2.6.32-504.23.4.el6

noarch
kernel-doc-2.6.32-504.23.4.el6
kernel-firmware-2.6.32-504.23.4.el6
kernel-abi-whitelists-2.6.32-504.23.4.el6

x86_64
kernel-debuginfo-common-x86_64-2.6.32-504.23.4.el6
kernel-headers-2.6.32-504.23.4.el6
python-perf-debuginfo-2.6.32-504.23.4.el6
kernel-2.6.32-504.23.4.el6
kernel-debug-devel-2.6.32-504.23.4.el6
kernel-debug-debuginfo-2.6.32-504.23.4.el6

kernel-debug-2.6.32-504.23.4.el6
perf-debuginfo-2.6.32-504.23.4.el6
kernel-debuginfo-2.6.32-504.23.4.el6
perf-2.6.32-504.23.4.el6
kernel-devel-2.6.32-504.23.4.el6
python-perf-2.6.32-504.23.4.el6

178087 - Gentoo Linux GLSA-201509-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3143, CVE-2015-3144, CVE-2015-3145, CVE-2015-3148, CVE-2015-3236, CVE-2015-3237

Description

The scan detected that the host is missing the following update:
GLSA-201509-02

Observation

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

https://security.gentoo.org/glsa/201509-02

Affected packages:
net-misc/curl < 7.43.0

178128 - Gentoo Linux GLSA-201507-16 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2100

Description

The scan detected that the host is missing the following update:
GLSA-201507-16

Observation

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

https://security.gentoo.org/glsa/201507-16

Affected packages:
sys-apps/portage < 2.1.12.2

19357 - NVIDIA Windows Drivers Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-7865, CVE-2015-7866, CVE-2015-7869, CVE-2015-8328

Description

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers.

Observation

NVIDIA is a technology company which manufactures graphics processing unit.

Multiple vulnerabilities are present in some versions of the NVIDIA Drivers. The flaws occur within multiple components. Successful exploitation could allow an attacker to cause a denial of service or bypass security restrictions and escalate privileges.

19436 - (ESA-2015-171) EMC NetWorker Denial of Service Vulnerability

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

Risk Level: High

CVE: CVE-2015-6849

Description

A denial of service vulnerability is present in some versions of EMC NetWorker.

Observation

EMC NetWorker is an enterprise backup and recovery solution.

A denial of service vulnerability is present in some versions of EMC NetWorker. The flaw lies in the RPC protocol authentication implementation. Successful exploitation could allow an attacker to cause a denial of service condition.

19441 - (SB10141) McAfee ePolicy Orchestrator Multiple Java Vulnerabilities

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

Risk Level: High

CVE: CVE-2015-4803, CVE-2015-4868, CVE-2015-4872, CVE-2015-4893, CVE-2015-4911

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws lie in the Java components. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

170591 - Amazon Linux AMI ALAS-2015-625 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5600, CVE-2015-6563, CVE-2015-6564

Description

The scan detected that the host is missing the following update:
ALAS-2015-625

Observation

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

https://alas.aws.amazon.com/ALAS-2015-625.html

Amazon Linux AMI
x86_64
openssh-debuginfo-6.6.1p1-22.58.amzn1
openssh-6.6.1p1-22.58.amzn1
pam_ssh_agent_auth-0.9.3-9.22.58.amzn1
openssh-clients-6.6.1p1-22.58.amzn1
openssh-keycat-6.6.1p1-22.58.amzn1
openssh-ldap-6.6.1p1-22.58.amzn1
openssh-server-6.6.1p1-22.58.amzn1

i686
openssh-debuginfo-6.6.1p1-22.58.amzn1
openssh-6.6.1p1-22.58.amzn1
pam_ssh_agent_auth-0.9.3-9.22.58.amzn1
openssh-clients-6.6.1p1-22.58.amzn1
openssh-keycat-6.6.1p1-22.58.amzn1
openssh-ldap-6.6.1p1-22.58.amzn1
openssh-server-6.6.1p1-22.58.amzn1

174711 - Scientific Linux Security ERRATA Important: libXfont on SL6.x, SL7.x i386/x86_64 (1509-6185)

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

Risk Level: High

CVE: CVE-2015-1802, CVE-2015-1803, CVE-2015-1804

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libXfont on SL6.x, SL7.x i386/x86_64 (1509-6185)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=6185

SL7
x86_64
libXfont-devel-1.4.7-3.el7_1
libXfont-debuginfo-1.4.7-3.el7_1
libXfont-1.4.7-3.el7_1

SL6
x86_64
libXfont-devel-1.4.5-5.el6_7
libXfont-debuginfo-1.4.5-5.el6_7
libXfont-1.4.5-5.el6_7

i386
libXfont-devel-1.4.5-5.el6_7
libXfont-debuginfo-1.4.5-5.el6_7
libXfont-1.4.5-5.el6_7

174733 - Scientific Linux Security ERRATA Important: pcs on SL6.x, SL7.x i386/x86_64 (1509-5495)

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

Risk Level: High

CVE: CVE-2015-5189, CVE-2015-5190

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: pcs on SL6.x, SL7.x i386/x86_64 (1509-5495)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=5495

SL7
x86_64
pcs-0.9.137-13.el7_1.4
pcs-debuginfo-0.9.137-13.el7_1.4
python-clufter-0.9.137-13.el7_1.4

SL6
x86_64
pcs-0.9.139-9.el6_7.1
pcs-debuginfo-0.9.139-9.el6_7.1

i386
pcs-0.9.139-9.el6_7.1
pcs-debuginfo-0.9.139-9.el6_7.1

178088 - Gentoo Linux GLSA-201507-21 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1802, CVE-2015-1803, CVE-2015-1804

Description

The scan detected that the host is missing the following update:
GLSA-201507-21

Observation

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

https://security.gentoo.org/glsa/201507-21

Affected packages:
x11-libs/libXfont < 1.5.1

19315 - TECO SG2 Client Multiple Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of TECO SG2 Client.

Observation

TECO SG2 Client is an application used for connecting and programming SG2 Smart Relay devices.

Multiple vulnerabilities are present in some versions of TECO SG2 Client. The flaws lie in the handling of GEN and GFB files. Successful exploitation could allow an attacker to remotely execute arbitrary code or to cause a denial of service condition.

19431 - (HPSBGN03430) HP ArcSight Logger Local Elevation Of Privilege Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6030

Description

A vulnerability is present in some versions of HP ArcSight Logger.

Observation

HP ArcSight Logger is a log analysis and management software.

A privilege escalation vulnerability is present in some versions of HP ArcSight Logger. The flaw lies in the root account that can be used to execute files owned by ArcSight.

19432 - (HT205639) Apple Safari Multiple Vulnerabilities Prior To 9.0.2

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

Risk Level: High

CVE: CVE-2015-7048, CVE-2015-7050, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, CVE-2015-7103, CVE-2015-7104

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in WebKit component. Successful exploitation could allow an attacker to obtain sensitive information, to cause denial of service or to execute arbitrary code.

88726 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-349-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
SSA:2015-349-02

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.504203

Slackware 14.0
x86_64
libpng-1.4.18-x86_64-1

Slackware 13.0
x86_64
libpng-1.2.55-x86_64-1

Slackware 13.1
x86_64
libpng-1.4.18-x86_64-1

Slackware 14.1
x86_64
libpng-1.4.18-x86_64-1

Slackware 13.37
x86_64
libpng-1.4.18-x86_64-1

91978 - Oracle Enterprise Linux ELSA-2015-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
ELSA-2015-2595

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005616.html

OEL7
x86_64
libpng12-devel-1.2.50-7.el7_2
libpng12-1.2.50-7.el7_2

91980 - Oracle Enterprise Linux ELSA-2015-2617 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8176, CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-3216, CVE-2015-4000

Description

The scan detected that the host is missing the following update:
ELSA-2015-2617

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005624.html
http://oss.oracle.com/pipermail/el-errata/2015-December/005625.html

OEL7
x86_64
openssl-static-1.0.1e-51.el7_2.1
openssl-devel-1.0.1e-51.el7_2.1
openssl-1.0.1e-51.el7_2.1
openssl-perl-1.0.1e-51.el7_2.1
openssl-libs-1.0.1e-51.el7_2.1

OEL6
x86_64
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

i386
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

91981 - Oracle Enterprise Linux ELSA-2015-2594 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
ELSA-2015-2594

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005617.html

OEL6
x86_64
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

i386
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

91982 - Oracle Enterprise Linux ELSA-2015-2596 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
ELSA-2015-2596

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005615.html

OEL7
x86_64
libpng-1.5.13-7.el7_2
libpng-static-1.5.13-7.el7_2
libpng-devel-1.5.13-7.el7_2

132205 - Oracle VM OVMSA-2015-0153 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0153

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-December/000401.html

OVM3.3
x86_64
libpng-1.2.49-2.el6_7

141032 - Red Hat Enterprise Linux RHSA-2015-2596 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
RHSA-2015-2596

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2596.html

RHEL7D
x86_64
libpng-debuginfo-1.5.13-7.el7_2
libpng-1.5.13-7.el7_2
libpng-static-1.5.13-7.el7_2
libpng-devel-1.5.13-7.el7_2

RHEL7WS
x86_64
libpng-debuginfo-1.5.13-7.el7_2
libpng-1.5.13-7.el7_2
libpng-static-1.5.13-7.el7_2
libpng-devel-1.5.13-7.el7_2

141038 - Red Hat Enterprise Linux RHSA-2015-2594 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
RHSA-2015-2594

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2594.html

RHEL6D
x86_64
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

i386
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

RHEL6S
i386
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

x86_64
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

RHEL6WS
x86_64

libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7

i386
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7

141041 - Red Hat Enterprise Linux RHSA-2015-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
RHSA-2015-2595

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2595.html

RHEL7D
x86_64
libpng12-debuginfo-1.2.50-7.el7_2
libpng12-1.2.50-7.el7_2
libpng12-devel-1.2.50-7.el7_2

RHEL7WS
x86_64
libpng12-debuginfo-1.2.50-7.el7_2
libpng12-1.2.50-7.el7_2
libpng12-devel-1.2.50-7.el7_2

144084 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2245-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-4514, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2245-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00049.html

SuSE Linux 13.1
x86_64

MozillaThunderbird-translations-other-38.4.0-70.68.1
MozillaThunderbird-devel-38.4.0-70.68.1
MozillaThunderbird-debuginfo-38.4.0-70.68.1
MozillaThunderbird-buildsymbols-38.4.0-70.68.1
MozillaThunderbird-38.4.0-70.68.1
MozillaThunderbird-translations-common-38.4.0-70.68.1
MozillaThunderbird-debugsource-38.4.0-70.68.1

i586
MozillaThunderbird-translations-other-38.4.0-70.68.1
MozillaThunderbird-devel-38.4.0-70.68.1
MozillaThunderbird-debuginfo-38.4.0-70.68.1
MozillaThunderbird-buildsymbols-38.4.0-70.68.1
MozillaThunderbird-38.4.0-70.68.1
MozillaThunderbird-translations-common-38.4.0-70.68.1
MozillaThunderbird-debugsource-38.4.0-70.68.1

SuSE Linux 13.2
x86_64
MozillaThunderbird-debugsource-38.4.0-31.1
MozillaThunderbird-devel-38.4.0-31.1
MozillaThunderbird-translations-common-38.4.0-31.1
MozillaThunderbird-translations-other-38.4.0-31.1
MozillaThunderbird-38.4.0-31.1
MozillaThunderbird-debuginfo-38.4.0-31.1
MozillaThunderbird-buildsymbols-38.4.0-31.1

i586
MozillaThunderbird-debugsource-38.4.0-31.1
MozillaThunderbird-devel-38.4.0-31.1
MozillaThunderbird-translations-common-38.4.0-31.1
MozillaThunderbird-translations-other-38.4.0-31.1
MozillaThunderbird-38.4.0-31.1
MozillaThunderbird-debuginfo-38.4.0-31.1
MozillaThunderbird-buildsymbols-38.4.0-31.1

144087 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2263-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2263-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00063.html

SuSE Linux 13.1
x86_64
libpng12-compat-devel-1.2.50-6.10.1
libpng12-0-32bit-1.2.50-6.10.1
libpng12-0-debuginfo-1.2.50-6.10.1
libpng12-devel-32bit-1.2.50-6.10.1

libpng12-0-1.2.50-6.10.1
libpng12-devel-1.2.50-6.10.1
libpng12-debugsource-1.2.50-6.10.1
libpng12-compat-devel-32bit-1.2.50-6.10.1
libpng12-0-debuginfo-32bit-1.2.50-6.10.1

i586
libpng12-0-debuginfo-1.2.50-6.10.1
libpng12-debugsource-1.2.50-6.10.1
libpng12-devel-1.2.50-6.10.1
libpng12-compat-devel-1.2.50-6.10.1
libpng12-0-1.2.50-6.10.1

SuSE Linux 13.2
x86_64
libpng12-0-debuginfo-32bit-1.2.51-3.6.1
libpng12-devel-1.2.51-3.6.1
libpng12-0-1.2.51-3.6.1
libpng12-compat-devel-32bit-1.2.51-3.6.1
libpng12-0-32bit-1.2.51-3.6.1
libpng12-devel-32bit-1.2.51-3.6.1
libpng12-debugsource-1.2.51-3.6.1
libpng12-0-debuginfo-1.2.51-3.6.1
libpng12-compat-devel-1.2.51-3.6.1

i586
libpng12-0-1.2.51-3.6.1
libpng12-debugsource-1.2.51-3.6.1
libpng12-devel-1.2.51-3.6.1
libpng12-compat-devel-1.2.51-3.6.1
libpng12-0-debuginfo-1.2.51-3.6.1

144088 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2262-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2262-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00062.html

SuSE Linux 13.1
x86_64
libpng16-16-debuginfo-1.6.6-22.1
libpng16-compat-devel-32bit-1.6.6-22.1
libpng16-tools-debuginfo-1.6.6-22.1
libpng16-debugsource-1.6.6-22.1
libpng16-16-32bit-1.6.6-22.1
libpng16-tools-1.6.6-22.1
libpng16-compat-devel-1.6.6-22.1
libpng16-16-debuginfo-32bit-1.6.6-22.1

libpng16-devel-1.6.6-22.1
libpng16-devel-32bit-1.6.6-22.1
libpng16-16-1.6.6-22.1

i586
libpng16-16-debuginfo-1.6.6-22.1
libpng16-tools-debuginfo-1.6.6-22.1
libpng16-debugsource-1.6.6-22.1
libpng16-tools-1.6.6-22.1
libpng16-compat-devel-1.6.6-22.1
libpng16-devel-1.6.6-22.1
libpng16-16-1.6.6-22.1

SuSE Linux 13.2
x86_64
libpng16-tools-debuginfo-1.6.13-2.10.1
libpng16-16-1.6.13-2.10.1
libpng16-tools-1.6.13-2.10.1
libpng16-devel-32bit-1.6.13-2.10.1
libpng16-debugsource-1.6.13-2.10.1
libpng16-devel-1.6.13-2.10.1
libpng16-16-debuginfo-32bit-1.6.13-2.10.1
libpng16-compat-devel-1.6.13-2.10.1
libpng16-16-32bit-1.6.13-2.10.1
libpng16-compat-devel-32bit-1.6.13-2.10.1
libpng16-16-debuginfo-1.6.13-2.10.1

i586
libpng16-tools-debuginfo-1.6.13-2.10.1
libpng16-16-1.6.13-2.10.1
libpng16-tools-1.6.13-2.10.1
libpng16-debugsource-1.6.13-2.10.1
libpng16-devel-1.6.13-2.10.1
libpng16-compat-devel-1.6.13-2.10.1
libpng16-16-debuginfo-1.6.13-2.10.1

144090 - SuSE Linux 13.2 openSUSE-SU-2015:2250-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5307, CVE-2015-7311, CVE-2015-7835, CVE-2015-7970, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2250-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00053.html

SuSE Linux 13.2
x86_64
xen-debugsource-4.4.3_04-33.1
xen-kmp-default-debuginfo-4.4.3_04_k3.16.7_29-33.1
xen-tools-4.4.3_04-33.1
xen-tools-domU-debuginfo-4.4.3_04-33.1

xen-tools-domU-4.4.3_04-33.1
xen-libs-4.4.3_04-33.1
xen-kmp-default-4.4.3_04_k3.16.7_29-33.1
xen-tools-debuginfo-4.4.3_04-33.1
xen-libs-32bit-4.4.3_04-33.1
xen-kmp-desktop-4.4.3_04_k3.16.7_29-33.1
xen-libs-debuginfo-32bit-4.4.3_04-33.1
xen-4.4.3_04-33.1
xen-doc-html-4.4.3_04-33.1
xen-libs-debuginfo-4.4.3_04-33.1
xen-kmp-desktop-debuginfo-4.4.3_04_k3.16.7_29-33.1
xen-devel-4.4.3_04-33.1

i586
xen-devel-4.4.3_04-33.1
xen-libs-4.4.3_04-33.1
xen-tools-domU-debuginfo-4.4.3_04-33.1
xen-tools-domU-4.4.3_04-33.1
xen-libs-debuginfo-4.4.3_04-33.1
xen-debugsource-4.4.3_04-33.1

144092 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2243-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0286, CVE-2015-0288, CVE-2015-1789, CVE-2015-1793, CVE-2015-3152, CVE-2015-4730, CVE-2015-4766, CVE-2015-4792, CVE-2015-4800, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4833, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4862, CVE-2015-4864, CVE-2015-4866, CVE-2015-4870, CVE-2015-4879, CVE-2015-4890, CVE-2015-4895, CVE-2015-4904, CVE-2015-4905, CVE-2015-4910, CVE-2015-4913

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2243-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00047.html

SuSE Linux 13.1
x86_64
mysql-community-server-client-debuginfo-5.6.27-7.13.1
mysql-community-server-test-debuginfo-5.6.27-7.13.1
libmysql56client_r18-32bit-5.6.27-7.13.1
mysql-community-server-errormessages-5.6.27-7.13.1
libmysql56client18-32bit-5.6.27-7.13.1
mysql-community-server-debugsource-5.6.27-7.13.1
mysql-community-server-test-5.6.27-7.13.1
libmysql56client18-debuginfo-32bit-5.6.27-7.13.1
mysql-community-server-tools-5.6.27-7.13.1
libmysql56client18-debuginfo-5.6.27-7.13.1
mysql-community-server-bench-5.6.27-7.13.1
mysql-community-server-tools-debuginfo-5.6.27-7.13.1
libmysql56client_r18-5.6.27-7.13.1
mysql-community-server-bench-debuginfo-5.6.27-7.13.1
mysql-community-server-debuginfo-5.6.27-7.13.1
libmysql56client18-5.6.27-7.13.1

mysql-community-server-5.6.27-7.13.1
mysql-community-server-client-5.6.27-7.13.1

i586
mysql-community-server-client-debuginfo-5.6.27-7.13.1
mysql-community-server-test-debuginfo-5.6.27-7.13.1
mysql-community-server-errormessages-5.6.27-7.13.1
mysql-community-server-debugsource-5.6.27-7.13.1
mysql-community-server-test-5.6.27-7.13.1
mysql-community-server-tools-5.6.27-7.13.1
libmysql56client18-debuginfo-5.6.27-7.13.1
mysql-community-server-bench-5.6.27-7.13.1
mysql-community-server-tools-debuginfo-5.6.27-7.13.1
libmysql56client_r18-5.6.27-7.13.1
mysql-community-server-bench-debuginfo-5.6.27-7.13.1
mysql-community-server-debuginfo-5.6.27-7.13.1
libmysql56client18-5.6.27-7.13.1
mysql-community-server-5.6.27-7.13.1
mysql-community-server-client-5.6.27-7.13.1

SuSE Linux 13.2
x86_64
mysql-community-server-debuginfo-5.6.27-2.12.1
libmysql56client_r18-32bit-5.6.27-2.12.1
mysql-community-server-5.6.27-2.12.1
libmysql56client18-5.6.27-2.12.1
mysql-community-server-bench-5.6.27-2.12.1
libmysql56client18-debuginfo-5.6.27-2.12.1
mysql-community-server-tools-5.6.27-2.12.1
mysql-community-server-test-5.6.27-2.12.1
libmysql56client18-32bit-5.6.27-2.12.1
libmysql56client18-debuginfo-32bit-5.6.27-2.12.1
mysql-community-server-errormessages-5.6.27-2.12.1
libmysql56client_r18-5.6.27-2.12.1
mysql-community-server-debugsource-5.6.27-2.12.1
mysql-community-server-test-debuginfo-5.6.27-2.12.1
mysql-community-server-client-5.6.27-2.12.1
mysql-community-server-client-debuginfo-5.6.27-2.12.1
mysql-community-server-tools-debuginfo-5.6.27-2.12.1
mysql-community-server-bench-debuginfo-5.6.27-2.12.1

i586
mysql-community-server-debuginfo-5.6.27-2.12.1
mysql-community-server-5.6.27-2.12.1
libmysql56client18-5.6.27-2.12.1
mysql-community-server-bench-5.6.27-2.12.1
libmysql56client18-debuginfo-5.6.27-2.12.1
mysql-community-server-tools-5.6.27-2.12.1
mysql-community-server-test-5.6.27-2.12.1
mysql-community-server-errormessages-5.6.27-2.12.1
libmysql56client_r18-5.6.27-2.12.1
mysql-community-server-debugsource-5.6.27-2.12.1
mysql-community-server-test-debuginfo-5.6.27-2.12.1
mysql-community-server-client-5.6.27-2.12.1
mysql-community-server-client-debuginfo-5.6.27-2.12.1
mysql-community-server-tools-debuginfo-5.6.27-2.12.1
mysql-community-server-bench-debuginfo-5.6.27-2.12.1

160013 - CentOS 6 CESA-2015-2594 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
CESA-2015-2594

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021517.html

CentOS 6
x86_64
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

i686
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

170594 - Amazon Linux AMI ALAS-2015-620 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

Description

The scan detected that the host is missing the following update:
ALAS-2015-620

Observation

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

https://alas.aws.amazon.com/ALAS-2015-620.html

Amazon Linux AMI
x86_64
binutils-devel-2.23.52.0.1-55.65.amzn1
binutils-2.23.52.0.1-55.65.amzn1
binutils-debuginfo-2.23.52.0.1-55.65.amzn1

i686
binutils-devel-2.23.52.0.1-55.65.amzn1
binutils-2.23.52.0.1-55.65.amzn1
binutils-debuginfo-2.23.52.0.1-55.65.amzn1

170597 - Amazon Linux AMI ALAS-2015-623 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8240, CVE-2014-8241

Description

The scan detected that the host is missing the following update:
ALAS-2015-623

Observation

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

https://alas.aws.amazon.com/ALAS-2015-623.html

Amazon Linux AMI
x86_64
tigervnc-debuginfo-1.3.1-3.31.amzn1
tigervnc-1.3.1-3.31.amzn1
tigervnc-server-1.3.1-3.31.amzn1
tigervnc-server-module-1.3.1-3.31.amzn1

i686
tigervnc-debuginfo-1.3.1-3.31.amzn1
tigervnc-1.3.1-3.31.amzn1
tigervnc-server-1.3.1-3.31.amzn1
tigervnc-server-module-1.3.1-3.31.amzn1

170600 - Amazon Linux AMI ALAS-2015-630 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8557

Description

The scan detected that the host is missing the following update:
ALAS-2015-630

Observation

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

https://alas.aws.amazon.com/ALAS-2015-630.html

Amazon Linux AMI
noarch
python27-pygments-1.4-4.12.amzn1
python26-pygments-1.4-4.12.amzn1

170605 - Amazon Linux AMI ALAS-2015-617 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7423, CVE-2015-1472, CVE-2015-1473, CVE-2015-1781, CVE-2015-5277

Description

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

ALAS-2015-617

Observation

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

https://alas.aws.amazon.com/ALAS-2015-617.html

Amazon Linux AMI
x86_64
glibc-devel-2.17-106.163.amzn1
glibc-debuginfo-2.17-106.163.amzn1
glibc-utils-2.17-106.163.amzn1
glibc-static-2.17-106.163.amzn1
glibc-headers-2.17-106.163.amzn1
glibc-common-2.17-106.163.amzn1
glibc-2.17-106.163.amzn1
glibc-debuginfo-common-2.17-106.163.amzn1
nscd-2.17-106.163.amzn1

i686
glibc-devel-2.17-106.163.amzn1
glibc-debuginfo-2.17-106.163.amzn1
glibc-utils-2.17-106.163.amzn1
glibc-static-2.17-106.163.amzn1
glibc-2.17-106.163.amzn1
glibc-common-2.17-106.163.amzn1
glibc-debuginfo-common-2.17-106.163.amzn1
glibc-headers-2.17-106.163.amzn1
nscd-2.17-106.163.amzn1

170607 - Amazon Linux AMI ALAS-2015-618 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
ALAS-2015-618

Observation

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

https://alas.aws.amazon.com/ALAS-2015-618.html

Amazon Linux AMI
noarch
apache-commons-collections-testframework-3.2.1-11.9.amzn1
apache-commons-collections-javadoc-3.2.1-11.9.amzn1
apache-commons-collections-3.2.1-11.9.amzn1
apache-commons-collections-testframework-javadoc-3.2.1-11.9.amzn1

174710 - Scientific Linux Security ERRATA Important: spice on SL7.x x86_64 (1510-614)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice on SL7.x x86_64 (1510-614)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=614

SL7
x86_64
spice-server-devel-0.12.4-9.el7_1.3
spice-server-0.12.4-9.el7_1.3
spice-debuginfo-0.12.4-9.el7_1.3

174712 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1506-5862)

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

Risk Level: High

CVE: CVE-2015-3209

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1506-5862)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=5862

SL6
x86_64
qemu-kvm-0.12.1.2-2.448.el6_6.4
qemu-guest-agent-0.12.1.2-2.448.el6_6.4
qemu-kvm-debuginfo-0.12.1.2-2.448.el6_6.4
qemu-kvm-tools-0.12.1.2-2.448.el6_6.4
qemu-img-0.12.1.2-2.448.el6_6.4

i386
qemu-guest-agent-0.12.1.2-2.448.el6_6.4
qemu-kvm-debuginfo-0.12.1.2-2.448.el6_6.4

174715 - Scientific Linux Security ERRATA Important: bind on SL5.x i386/x86_64 (1509-7220)

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

Risk Level: High

CVE: CVE-2015-5722

Description

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

Security ERRATA Important: bind on SL5.x i386/x86_64 (1509-7220)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=7220

SL5
x86_64
bind-chroot-9.3.6-25.P1.el5_11.4
bind-libs-9.3.6-25.P1.el5_11.4
bind-devel-9.3.6-25.P1.el5_11.4
bind-utils-9.3.6-25.P1.el5_11.4
bind-sdb-9.3.6-25.P1.el5_11.4
caching-nameserver-9.3.6-25.P1.el5_11.4
bind-debuginfo-9.3.6-25.P1.el5_11.4
bind-libbind-devel-9.3.6-25.P1.el5_11.4
bind-9.3.6-25.P1.el5_11.4

i386
bind-chroot-9.3.6-25.P1.el5_11.4
bind-libs-9.3.6-25.P1.el5_11.4
bind-devel-9.3.6-25.P1.el5_11.4
bind-utils-9.3.6-25.P1.el5_11.4
bind-sdb-9.3.6-25.P1.el5_11.4
caching-nameserver-9.3.6-25.P1.el5_11.4
bind-debuginfo-9.3.6-25.P1.el5_11.4
bind-libbind-devel-9.3.6-25.P1.el5_11.4
bind-9.3.6-25.P1.el5_11.4

174716 - Scientific Linux Security ERRATA Important: ntp on SL6.x, SL7.x i386/x86_64 (1510-5166)

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

Risk Level: High

CVE: CVE-2015-5300, CVE-2015-7704

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: ntp on SL6.x, SL7.x i386/x86_64 (1510-5166)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=5166

SL7
x86_64
ntpdate-4.2.6p5-19.el7_1.3
sntp-4.2.6p5-19.el7_1.3
ntp-4.2.6p5-19.el7_1.3
ntp-debuginfo-4.2.6p5-19.el7_1.3

noarch
ntp-doc-4.2.6p5-19.el7_1.3
ntp-perl-4.2.6p5-19.el7_1.3

SL6
i386
ntp-perl-4.2.6p5-5.el6_7.2
ntp-debuginfo-4.2.6p5-5.el6_7.2
ntp-4.2.6p5-5.el6_7.2
ntpdate-4.2.6p5-5.el6_7.2

noarch
ntp-doc-4.2.6p5-5.el6_7.2

x86_64
ntp-perl-4.2.6p5-5.el6_7.2
ntp-debuginfo-4.2.6p5-5.el6_7.2
ntp-4.2.6p5-5.el6_7.2
ntpdate-4.2.6p5-5.el6_7.2

174722 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1509-6559)

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

Risk Level: High

CVE: CVE-2015-5722

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1509-6559)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=6559

SL5
x86_64
bind97-9.7.0-21.P2.el5_11.3
bind97-chroot-9.7.0-21.P2.el5_11.3
bind97-libs-9.7.0-21.P2.el5_11.3
bind97-utils-9.7.0-21.P2.el5_11.3
bind97-debuginfo-9.7.0-21.P2.el5_11.3
bind97-devel-9.7.0-21.P2.el5_11.3

i386
bind97-9.7.0-21.P2.el5_11.3
bind97-chroot-9.7.0-21.P2.el5_11.3
bind97-libs-9.7.0-21.P2.el5_11.3
bind97-utils-9.7.0-21.P2.el5_11.3
bind97-debuginfo-9.7.0-21.P2.el5_11.3
bind97-devel-9.7.0-21.P2.el5_11.3

174725 - Scientific Linux Security ERRATA Moderate: freeradius on SL6.x i386/x86_64 (1508-6517)

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

Risk Level: High

CVE: CVE-2014-2015

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: freeradius on SL6.x i386/x86_64 (1508-6517)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=6517

SL6
x86_64
freeradius-utils-2.2.6-4.el6
freeradius-debuginfo-2.2.6-4.el6
freeradius-postgresql-2.2.6-4.el6
freeradius-ldap-2.2.6-4.el6
freeradius-krb5-2.2.6-4.el6
freeradius-2.2.6-4.el6
freeradius-perl-2.2.6-4.el6
freeradius-unixODBC-2.2.6-4.el6
freeradius-mysql-2.2.6-4.el6
freeradius-python-2.2.6-4.el6

i386
freeradius-utils-2.2.6-4.el6
freeradius-debuginfo-2.2.6-4.el6
freeradius-postgresql-2.2.6-4.el6
freeradius-ldap-2.2.6-4.el6
freeradius-krb5-2.2.6-4.el6
freeradius-2.2.6-4.el6
freeradius-perl-2.2.6-4.el6
freeradius-unixODBC-2.2.6-4.el6
freeradius-mysql-2.2.6-4.el6
freeradius-python-2.2.6-4.el6

174726 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-813)

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-813)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=813

SL5
x86_64
firefox-debuginfo-38.4.0-1.el5_11
firefox-38.4.0-1.el5_11

i386

firefox-debuginfo-38.4.0-1.el5_11
firefox-38.4.0-1.el5_11

SL7
x86_64
firefox-debuginfo-38.4.0-1.el7_1
firefox-38.4.0-1.el7_1

SL6
x86_64
firefox-38.4.0-1.el6_7
firefox-debuginfo-38.4.0-1.el6_7

i386
firefox-38.4.0-1.el6_7
firefox-debuginfo-38.4.0-1.el6_7

174728 - Scientific Linux Security ERRATA Moderate: mailman on SL6.x i386/x86_64 (1508-1781)

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

Risk Level: High

CVE: CVE-2002-0389, CVE-2015-2775

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: mailman on SL6.x i386/x86_64 (1508-1781)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=1781

SL6
x86_64
mailman-2.1.12-25.el6
mailman-debuginfo-2.1.12-25.el6

i386
mailman-2.1.12-25.el6
mailman-debuginfo-2.1.12-25.el6

174729 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1509-16762)

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

Risk Level: High

CVE: CVE-2015-4500, CVE-2015-4509, CVE-2015-4510

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1509-16762)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=16762

SL5
x86_64
firefox-debuginfo-38.3.0-2.el5_11
firefox-38.3.0-2.el5_11

i386
firefox-debuginfo-38.3.0-2.el5_11
firefox-38.3.0-2.el5_11

SL7
x86_64
firefox-debuginfo-38.3.0-2.el7_1
firefox-38.3.0-2.el7_1

SL6
x86_64
firefox-debuginfo-38.3.0-2.el6_7
firefox-38.3.0-2.el6_7

i386
firefox-debuginfo-38.3.0-2.el6_7
firefox-38.3.0-2.el6_7

174731 - Scientific Linux Security ERRATA Important: kernel on SL5.x i386/x86_64 (1506-2521)

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

Risk Level: High

CVE: CVE-2015-1805

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL5.x i386/x86_64 (1506-2521)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=2521

SL5
i386
kernel-xen-2.6.18-406.el5
kernel-debug-debuginfo-2.6.18-406.el5
kernel-xen-debuginfo-2.6.18-406.el5
kernel-2.6.18-406.el5
kernel-PAE-2.6.18-406.el5
kernel-debuginfo-2.6.18-406.el5
kernel-xen-devel-2.6.18-406.el5
kernel-headers-2.6.18-406.el5
kernel-PAE-devel-2.6.18-406.el5
kernel-debuginfo-common-2.6.18-406.el5
kernel-PAE-debuginfo-2.6.18-406.el5
kernel-debug-2.6.18-406.el5
kernel-debug-devel-2.6.18-406.el5
kernel-devel-2.6.18-406.el5

noarch
kernel-doc-2.6.18-406.el5

x86_64
kernel-debug-devel-2.6.18-406.el5
kernel-debuginfo-2.6.18-406.el5
kernel-headers-2.6.18-406.el5
kernel-xen-debuginfo-2.6.18-406.el5
kernel-debug-debuginfo-2.6.18-406.el5
kernel-xen-2.6.18-406.el5
kernel-2.6.18-406.el5
kernel-debuginfo-common-2.6.18-406.el5
kernel-devel-2.6.18-406.el5
kernel-debug-2.6.18-406.el5
kernel-xen-devel-2.6.18-406.el5

174735 - Scientific Linux Security ERRATA Moderate: pacemaker on SL6.x i386/x86_64 (1508-4316)

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

Risk Level: High

CVE: CVE-2015-1867

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pacemaker on SL6.x i386/x86_64 (1508-4316)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=4316

SL6
x86_64
pacemaker-libs-1.1.12-8.el6
pacemaker-remote-1.1.12-8.el6
pacemaker-doc-1.1.12-8.el6
pacemaker-1.1.12-8.el6
pacemaker-cts-1.1.12-8.el6
pacemaker-debuginfo-1.1.12-8.el6
pacemaker-libs-devel-1.1.12-8.el6
pacemaker-cluster-libs-1.1.12-8.el6
pacemaker-cli-1.1.12-8.el6

i386
pacemaker-libs-1.1.12-8.el6
pacemaker-remote-1.1.12-8.el6
pacemaker-doc-1.1.12-8.el6
pacemaker-1.1.12-8.el6
pacemaker-cts-1.1.12-8.el6
pacemaker-debuginfo-1.1.12-8.el6
pacemaker-libs-devel-1.1.12-8.el6
pacemaker-cluster-libs-1.1.12-8.el6
pacemaker-cli-1.1.12-8.el6

174736 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1510-78)

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

Risk Level: High

CVE: CVE-2015-4500, CVE-2015-4509, CVE-2015-4517, CVE-2015-4519, CVE-2015-4520, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1510-78)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=78

SL5
x86_64
thunderbird-38.3.0-1.el5_11
thunderbird-debuginfo-38.3.0-1.el5_11

i386
thunderbird-38.3.0-1.el5_11
thunderbird-debuginfo-38.3.0-1.el5_11

SL7
x86_64
thunderbird-38.3.0-1.el7_1
thunderbird-debuginfo-38.3.0-1.el7_1

SL6
x86_64
thunderbird-38.3.0-1.el6_7
thunderbird-debuginfo-38.3.0-1.el6_7

i386
thunderbird-38.3.0-1.el6_7
thunderbird-debuginfo-38.3.0-1.el6_7

174738 - Scientific Linux Security ERRATA Moderate: net-snmp on SL6.x, SL7.x i386/x86_64 (1508-17292)

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

Risk Level: High

CVE: CVE-2015-5621

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: net-snmp on SL6.x, SL7.x i386/x86_64 (1508-17292)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=17292

SL7
x86_64
net-snmp-gui-5.7.2-20.el7_1.1

net-snmp-agent-libs-5.7.2-20.el7_1.1
net-snmp-python-5.7.2-20.el7_1.1
net-snmp-sysvinit-5.7.2-20.el7_1.1
net-snmp-5.7.2-20.el7_1.1
net-snmp-libs-5.7.2-20.el7_1.1
net-snmp-debuginfo-5.7.2-20.el7_1.1
net-snmp-devel-5.7.2-20.el7_1.1
net-snmp-utils-5.7.2-20.el7_1.1
net-snmp-perl-5.7.2-20.el7_1.1

SL6
x86_64
net-snmp-python-5.5-54.el6_7.1
net-snmp-debuginfo-5.5-54.el6_7.1
net-snmp-5.5-54.el6_7.1
net-snmp-libs-5.5-54.el6_7.1
net-snmp-devel-5.5-54.el6_7.1
net-snmp-perl-5.5-54.el6_7.1
net-snmp-utils-5.5-54.el6_7.1

i386
net-snmp-python-5.5-54.el6_7.1
net-snmp-debuginfo-5.5-54.el6_7.1
net-snmp-5.5-54.el6_7.1
net-snmp-libs-5.5-54.el6_7.1
net-snmp-devel-5.5-54.el6_7.1
net-snmp-perl-5.5-54.el6_7.1
net-snmp-utils-5.5-54.el6_7.1

174741 - Scientific Linux Security ERRATA Important: jakarta-taglibs-standard on SL6.x, SL7.x (noarch) (1508-25222)

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

Risk Level: High

CVE: CVE-2015-0254

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: jakarta-taglibs-standard on SL6.x, SL7.x (noarch) (1508-25222)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=25222

SL7
noarch
jakarta-taglibs-standard-1.1.2-14.el7_1
jakarta-taglibs-standard-javadoc-1.1.2-14.el7_1

SL6
noarch
jakarta-taglibs-standard-1.1.1-11.7.el6_7
jakarta-taglibs-standard-javadoc-1.1.1-11.7.el6_7

174743 - Scientific Linux Security ERRATA Moderate: libpng on SL6.x i386/x86_64 (1512-559)

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libpng on SL6.x i386/x86_64 (1512-559)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=559

SL6
x86_64
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

i386
libpng-1.2.49-2.el6_7
libpng-devel-1.2.49-2.el6_7
libpng-debuginfo-1.2.49-2.el6_7
libpng-static-1.2.49-2.el6_7

174744 - Scientific Linux Security ERRATA Moderate: sqlite on SL7.x x86_64 (1508-15216)

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

Risk Level: High

CVE: CVE-2015-3414, CVE-2015-3415, CVE-2015-3416

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: sqlite on SL7.x x86_64 (1508-15216)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=15216

SL7
x86_64
lemon-3.7.17-6.el7_1.1
sqlite-3.7.17-6.el7_1.1
sqlite-tcl-3.7.17-6.el7_1.1
sqlite-devel-3.7.17-6.el7_1.1
sqlite-debuginfo-3.7.17-6.el7_1.1

noarch
sqlite-doc-3.7.17-6.el7_1.1

174746 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1508-14855)

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

Risk Level: High

CVE: CVE-2015-5364, CVE-2015-5366

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1508-14855)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=14855

SL6
i386
kernel-debug-devel-2.6.32-573.3.1.el6
perf-debuginfo-2.6.32-573.3.1.el6
perf-2.6.32-573.3.1.el6
kernel-debug-2.6.32-573.3.1.el6
kernel-headers-2.6.32-573.3.1.el6
kernel-debuginfo-2.6.32-573.3.1.el6
kernel-2.6.32-573.3.1.el6
kernel-devel-2.6.32-573.3.1.el6
python-perf-2.6.32-573.3.1.el6
python-perf-debuginfo-2.6.32-573.3.1.el6
kernel-debuginfo-common-i686-2.6.32-573.3.1.el6
kernel-debug-debuginfo-2.6.32-573.3.1.el6

noarch
kernel-firmware-2.6.32-573.3.1.el6
kernel-abi-whitelists-2.6.32-573.3.1.el6
kernel-doc-2.6.32-573.3.1.el6

x86_64
perf-2.6.32-573.3.1.el6
kernel-debug-devel-2.6.32-573.3.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.3.1.el6
kernel-debuginfo-common-i686-2.6.32-573.3.1.el6
kernel-devel-2.6.32-573.3.1.el6
kernel-debug-debuginfo-2.6.32-573.3.1.el6
python-perf-2.6.32-573.3.1.el6
kernel-debuginfo-2.6.32-573.3.1.el6
kernel-headers-2.6.32-573.3.1.el6
kernel-2.6.32-573.3.1.el6
kernel-debug-2.6.32-573.3.1.el6
python-perf-debuginfo-2.6.32-573.3.1.el6
perf-debuginfo-2.6.32-573.3.1.el6

174747 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1508-746)

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

Risk Level: High

CVE: CVE-2015-4620

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x i386/x86_64 (1508-746)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=746

SL6
x86_64
bind-9.8.2-0.37.rc1.el6_7.1
bind-libs-9.8.2-0.37.rc1.el6_7.1
bind-utils-9.8.2-0.37.rc1.el6_7.1
bind-debuginfo-9.8.2-0.37.rc1.el6_7.1
bind-sdb-9.8.2-0.37.rc1.el6_7.1
bind-devel-9.8.2-0.37.rc1.el6_7.1
bind-chroot-9.8.2-0.37.rc1.el6_7.1

i386
bind-9.8.2-0.37.rc1.el6_7.1
bind-libs-9.8.2-0.37.rc1.el6_7.1
bind-utils-9.8.2-0.37.rc1.el6_7.1
bind-debuginfo-9.8.2-0.37.rc1.el6_7.1
bind-sdb-9.8.2-0.37.rc1.el6_7.1
bind-devel-9.8.2-0.37.rc1.el6_7.1
bind-chroot-9.8.2-0.37.rc1.el6_7.1

174748 - Scientific Linux Security ERRATA Important: bind on SL6.x, SL7.x i386/x86_64 (1509-6888)

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

Risk Level: High

CVE: CVE-2015-5722

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x, SL7.x i386/x86_64 (1509-6888)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=6888

SL7
x86_64
bind-9.9.4-18.el7_1.5
bind-debuginfo-9.9.4-18.el7_1.5
bind-utils-9.9.4-18.el7_1.5
bind-libs-9.9.4-18.el7_1.5
bind-devel-9.9.4-18.el7_1.5
bind-lite-devel-9.9.4-18.el7_1.5
bind-libs-lite-9.9.4-18.el7_1.5
bind-chroot-9.9.4-18.el7_1.5
bind-sdb-chroot-9.9.4-18.el7_1.5
bind-sdb-9.9.4-18.el7_1.5

noarch
bind-license-9.9.4-18.el7_1.5

SL6
x86_64
bind-utils-9.8.2-0.37.rc1.el6_7.4
bind-9.8.2-0.37.rc1.el6_7.4
bind-chroot-9.8.2-0.37.rc1.el6_7.4
bind-debuginfo-9.8.2-0.37.rc1.el6_7.4
bind-devel-9.8.2-0.37.rc1.el6_7.4
bind-libs-9.8.2-0.37.rc1.el6_7.4
bind-sdb-9.8.2-0.37.rc1.el6_7.4

i386
bind-utils-9.8.2-0.37.rc1.el6_7.4
bind-9.8.2-0.37.rc1.el6_7.4
bind-chroot-9.8.2-0.37.rc1.el6_7.4
bind-debuginfo-9.8.2-0.37.rc1.el6_7.4
bind-devel-9.8.2-0.37.rc1.el6_7.4
bind-libs-9.8.2-0.37.rc1.el6_7.4
bind-sdb-9.8.2-0.37.rc1.el6_7.4

174751 - Scientific Linux Security ERRATA Important: bind on SL6.x, SL7.x i386/x86_64 (1508-77)

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

Risk Level: High

CVE: CVE-2015-5477

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL6.x, SL7.x i386/x86_64 (1508-77)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=77

SL7
x86_64
bind-utils-9.9.4-18.el7_1.3
bind-libs-lite-9.9.4-18.el7_1.3
bind-chroot-9.9.4-18.el7_1.3
bind-debuginfo-9.9.4-18.el7_1.3
bind-lite-devel-9.9.4-18.el7_1.3
bind-sdb-9.9.4-18.el7_1.3
bind-devel-9.9.4-18.el7_1.3
bind-9.9.4-18.el7_1.3
bind-sdb-chroot-9.9.4-18.el7_1.3
bind-libs-9.9.4-18.el7_1.3

noarch
bind-license-9.9.4-18.el7_1.3

SL6
x86_64
bind-9.8.2-0.37.rc1.el6_7.2
bind-debuginfo-9.8.2-0.37.rc1.el6_7.2
bind-utils-9.8.2-0.37.rc1.el6_7.2
bind-chroot-9.8.2-0.37.rc1.el6_7.2
bind-devel-9.8.2-0.37.rc1.el6_7.2

bind-libs-9.8.2-0.37.rc1.el6_7.2
bind-sdb-9.8.2-0.37.rc1.el6_7.2

i386
bind-9.8.2-0.37.rc1.el6_7.2
bind-debuginfo-9.8.2-0.37.rc1.el6_7.2
bind-utils-9.8.2-0.37.rc1.el6_7.2
bind-chroot-9.8.2-0.37.rc1.el6_7.2
bind-devel-9.8.2-0.37.rc1.el6_7.2
bind-libs-9.8.2-0.37.rc1.el6_7.2
bind-sdb-9.8.2-0.37.rc1.el6_7.2

174752 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1507-9033)

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

Risk Level: High

CVE: CVE-2015-4620

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL7.x x86_64 (1507-9033)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=9033

SL7
x86_64
bind-libs-lite-9.9.4-18.el7_1.2
bind-devel-9.9.4-18.el7_1.2
bind-sdb-9.9.4-18.el7_1.2
bind-debuginfo-9.9.4-18.el7_1.2
bind-chroot-9.9.4-18.el7_1.2
bind-libs-9.9.4-18.el7_1.2
bind-9.9.4-18.el7_1.2
bind-sdb-chroot-9.9.4-18.el7_1.2
bind-lite-devel-9.9.4-18.el7_1.2
bind-utils-9.9.4-18.el7_1.2

noarch
bind-license-9.9.4-18.el7_1.2

174754 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1509-15990)

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

Risk Level: High

CVE: CVE-2014-9585, CVE-2015-0275, CVE-2015-1333, CVE-2015-3212, CVE-2015-4700, CVE-2015-5364, CVE-2015-5366

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1509-15990)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=15990

SL7
x86_64
kernel-debug-debuginfo-3.10.0-229.14.1.el7
kernel-debug-3.10.0-229.14.1.el7
perf-debuginfo-3.10.0-229.14.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.14.1.el7
kernel-headers-3.10.0-229.14.1.el7
kernel-tools-libs-3.10.0-229.14.1.el7
kernel-3.10.0-229.14.1.el7
python-perf-3.10.0-229.14.1.el7
kernel-devel-3.10.0-229.14.1.el7
kernel-tools-3.10.0-229.14.1.el7
kernel-debuginfo-3.10.0-229.14.1.el7
perf-3.10.0-229.14.1.el7
kernel-tools-debuginfo-3.10.0-229.14.1.el7
kernel-debug-devel-3.10.0-229.14.1.el7
kernel-tools-libs-devel-3.10.0-229.14.1.el7
python-perf-debuginfo-3.10.0-229.14.1.el7

noarch
kernel-abi-whitelists-3.10.0-229.14.1.el7
kernel-doc-3.10.0-229.14.1.el7

174756 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1507-12261)

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

Risk Level: High

CVE: CVE-2015-3214, CVE-2015-5154

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1507-12261)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=12261

SL7
x86_64
libcacard-tools-1.5.3-86.el7_1.5
qemu-kvm-tools-1.5.3-86.el7_1.5
qemu-kvm-common-1.5.3-86.el7_1.5
qemu-img-1.5.3-86.el7_1.5
qemu-kvm-debuginfo-1.5.3-86.el7_1.5
qemu-kvm-1.5.3-86.el7_1.5
libcacard-1.5.3-86.el7_1.5
libcacard-devel-1.5.3-86.el7_1.5

174763 - Scientific Linux Security ERRATA moderate: Moderate: Openssl Security Update on SL6.x, SL7.x i386/srpm/x86_64 (1506-6990)

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

Risk Level: High

CVE: CVE-2014-8176, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-3216

Description

The scan detected that the host is missing the following update:
Security ERRATA moderate: Moderate: Openssl Security Update on SL6.x, SL7.x i386/srpm/x86_64 (1506-6990)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=6990

SL7
x86_64
openssl-debuginfo-1.0.1e-42.el7_1.8
openssl-static-1.0.1e-42.el7_1.8
openssl-1.0.1e-42.el7_1.8
openssl-devel-1.0.1e-42.el7_1.8
openssl-libs-1.0.1e-42.el7_1.8
openssl-perl-1.0.1e-42.el7_1.8

SL6
x86_64
openssl-static-1.0.1e-30.el6_6.11
openssl-devel-1.0.1e-30.el6_6.11
openssl-1.0.1e-30.el6_6.11
openssl-debuginfo-1.0.1e-30.el6_6.11
openssl-perl-1.0.1e-30.el6_6.11

i386
openssl-static-1.0.1e-30.el6_6.11
openssl-devel-1.0.1e-30.el6_6.11
openssl-1.0.1e-30.el6_6.11
openssl-debuginfo-1.0.1e-30.el6_6.11
openssl-perl-1.0.1e-30.el6_6.11

174764 - Scientific Linux Security ERRATA Important: abrt on SL7.x x86_64 (1506-6189)

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

Risk Level: High

CVE: CVE-2015-1869, CVE-2015-1870, CVE-2015-3142, CVE-2015-3147, CVE-2015-3150, CVE-2015-3151, CVE-2015-3159, CVE-2015-3315

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: abrt on SL7.x x86_64 (1506-6189)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=6189

SL7
x86_64

libreport-compat-2.1.11-23.sl7
libreport-devel-2.1.11-23.sl7
libreport-anaconda-2.1.11-23.sl7
libreport-plugin-bugzilla-2.1.11-23.sl7
abrt-dbus-2.1.11-22.el7_1
abrt-retrace-client-2.1.11-22.el7_1
abrt-debuginfo-2.1.11-22.el7_1
abrt-addon-pstoreoops-2.1.11-22.el7_1
abrt-desktop-2.1.11-22.el7_1
abrt-console-notification-2.1.11-22.el7_1
libreport-debuginfo-2.1.11-23.sl7
abrt-tui-2.1.11-22.el7_1
libreport-plugin-mailx-2.1.11-23.sl7
libreport-filesystem-2.1.11-23.sl7
libreport-2.1.11-23.sl7
abrt-addon-ccpp-2.1.11-22.el7_1
abrt-devel-2.1.11-22.el7_1
abrt-cli-2.1.11-22.el7_1
abrt-addon-python-2.1.11-22.el7_1
abrt-gui-devel-2.1.11-22.el7_1
abrt-addon-xorg-2.1.11-22.el7_1
libreport-newt-2.1.11-23.sl7
libreport-rhel-anaconda-bugzilla-2.1.11-23.sl7
libreport-plugin-reportuploader-2.1.11-23.sl7
libreport-rhel-bugzilla-2.1.11-23.sl7
libreport-gtk-devel-2.1.11-23.sl7
abrt-gui-libs-2.1.11-22.el7_1
libreport-rhel-2.1.11-23.sl7
libreport-gtk-2.1.11-23.sl7
abrt-addon-vmcore-2.1.11-22.el7_1
abrt-python-2.1.11-22.el7_1
abrt-gui-2.1.11-22.el7_1
libreport-cli-2.1.11-23.sl7
libreport-plugin-rhtsupport-2.1.11-23.sl7
libreport-web-devel-2.1.11-23.sl7
abrt-addon-kerneloops-2.1.11-22.el7_1
libreport-web-2.1.11-23.sl7
abrt-2.1.11-22.el7_1
abrt-libs-2.1.11-22.el7_1
libreport-plugin-logger-2.1.11-23.sl7
abrt-addon-upload-watch-2.1.11-22.el7_1
libreport-plugin-ureport-2.1.11-23.sl7
libreport-plugin-kerneloops-2.1.11-23.sl7
libreport-python-2.1.11-23.sl7

noarch
abrt-python-doc-2.1.11-22.el7_1

174766 - Scientific Linux Security ERRATA Critical: nss and nspr on SL5.x i386/x86_64 (1511-79)

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

Risk Level: High

CVE: CVE-2015-7181, CVE-2015-7182, CVE-2015-7183

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: nss and nspr on SL5.x i386/x86_64 (1511-79)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=79

SL5
x86_64
nspr-4.10.8-2.el5_11
nss-tools-3.19.1-2.el5_11
nspr-devel-4.10.8-2.el5_11
nss-devel-3.19.1-2.el5_11
nspr-debuginfo-4.10.8-2.el5_11
nss-pkcs11-devel-3.19.1-2.el5_11
nss-3.19.1-2.el5_11
nss-debuginfo-3.19.1-2.el5_11

i386
nspr-4.10.8-2.el5_11
nss-tools-3.19.1-2.el5_11
nspr-devel-4.10.8-2.el5_11
nss-devel-3.19.1-2.el5_11
nspr-debuginfo-4.10.8-2.el5_11
nss-pkcs11-devel-3.19.1-2.el5_11
nss-3.19.1-2.el5_11
nss-debuginfo-3.19.1-2.el5_11

174772 - Scientific Linux Security ERRATA Critical: nss, nss-util, and nspr on SL6.x, SL7.x i386/x86_64 (1511-1275)

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

Risk Level: High

CVE: CVE-2015-7181, CVE-2015-7182, CVE-2015-7183

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: nss, nss-util, and nspr on SL6.x, SL7.x i386/x86_64 (1511-1275)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=1275

SL7
x86_64
nss-util-debuginfo-3.19.1-4.el7_1
nspr-4.10.8-2.el7_1
nspr-debuginfo-4.10.8-2.el7_1
nss-tools-3.19.1-7.el7_1.2
nss-pkcs11-devel-3.19.1-7.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-devel-3.19.1-7.el7_1.2
nss-3.19.1-7.el7_1.2
nss-debuginfo-3.19.1-7.el7_1.2
nss-sysinit-3.19.1-7.el7_1.2
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

SL6
x86_64
nss-util-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

i386
nss-util-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

174776 - Scientific Linux Security ERRATA Important: bind on SL5.x i386/x86_64 (1507-13277)

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

Risk Level: High

CVE: CVE-2015-5477

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind on SL5.x i386/x86_64 (1507-13277)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=13277

SL5
x86_64
bind-debuginfo-9.3.6-25.P1.el5_11.3
bind-utils-9.3.6-25.P1.el5_11.3
caching-nameserver-9.3.6-25.P1.el5_11.3
bind-devel-9.3.6-25.P1.el5_11.3
bind-libbind-devel-9.3.6-25.P1.el5_11.3
bind-9.3.6-25.P1.el5_11.3
bind-sdb-9.3.6-25.P1.el5_11.3
bind-chroot-9.3.6-25.P1.el5_11.3
bind-libs-9.3.6-25.P1.el5_11.3

i386

bind-debuginfo-9.3.6-25.P1.el5_11.3
bind-utils-9.3.6-25.P1.el5_11.3
caching-nameserver-9.3.6-25.P1.el5_11.3
bind-devel-9.3.6-25.P1.el5_11.3
bind-libbind-devel-9.3.6-25.P1.el5_11.3
bind-9.3.6-25.P1.el5_11.3
bind-sdb-9.3.6-25.P1.el5_11.3
bind-chroot-9.3.6-25.P1.el5_11.3
bind-libs-9.3.6-25.P1.el5_11.3

174777 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1506-13468)

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

Risk Level: High

CVE: CVE-2014-9420, CVE-2014-9529, CVE-2014-9584, CVE-2015-1573, CVE-2015-1593, CVE-2015-1805, CVE-2015-2830

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1506-13468)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=13468

SL7
x86_64
kernel-tools-debuginfo-3.10.0-229.7.2.el7
kernel-tools-libs-3.10.0-229.7.2.el7
python-perf-debuginfo-3.10.0-229.7.2.el7
kernel-debug-debuginfo-3.10.0-229.7.2.el7
kernel-tools-libs-devel-3.10.0-229.7.2.el7
kernel-devel-3.10.0-229.7.2.el7
kernel-debuginfo-3.10.0-229.7.2.el7
python-perf-3.10.0-229.7.2.el7
perf-debuginfo-3.10.0-229.7.2.el7
kernel-3.10.0-229.7.2.el7
perf-3.10.0-229.7.2.el7
kernel-headers-3.10.0-229.7.2.el7
kernel-debug-3.10.0-229.7.2.el7
kernel-debug-devel-3.10.0-229.7.2.el7
kernel-debuginfo-common-x86_64-3.10.0-229.7.2.el7
kernel-tools-3.10.0-229.7.2.el7

noarch
kernel-abi-whitelists-3.10.0-229.7.2.el7
kernel-doc-3.10.0-229.7.2.el7

174778 - Scientific Linux Security ERRATA Important: spice-server on SL6.x x86_64 (1510-953)

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice-server on SL6.x x86_64 (1510-953)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=953

SL6
x86_64
spice-server-0.12.4-12.el6_7.3
spice-server-debuginfo-0.12.4-12.el6_7.3
spice-server-devel-0.12.4-12.el6_7.3

174783 - Scientific Linux Security ERRATA Important: kvm on SL5.x x86_64 (1506-14245)

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

Risk Level: High

CVE: CVE-2015-3209

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kvm on SL5.x x86_64 (1506-14245)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=14245

SL5
x86_64
kvm-tools-83-273.el5_11
kvm-qemu-img-83-273.el5_11
kvm-83-273.el5_11
kmod-kvm-debug-83-273.el5_11
kmod-kvm-83-273.el5_11
kvm-debuginfo-83-273.el5_11

174784 - Scientific Linux Security ERRATA Important: xen on SL5.x i386/x86_64 (1511-11464)

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

Risk Level: High

CVE: CVE-2015-5279

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: xen on SL5.x i386/x86_64 (1511-11464)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=11464

SL5
x86_64
xen-3.0.3-147.el5_11
xen-debuginfo-3.0.3-147.el5_11
xen-devel-3.0.3-147.el5_11
xen-libs-3.0.3-147.el5_11

i386
xen-3.0.3-147.el5_11
xen-debuginfo-3.0.3-147.el5_11
xen-devel-3.0.3-147.el5_11
xen-libs-3.0.3-147.el5_11

174787 - Scientific Linux Security ERRATA Moderate: mysql55-mysql on SL5.x i386/x86_64 (1508-16594)

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

Risk Level: High

CVE: CVE-2014-6568, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0391, CVE-2015-0411, CVE-2015-0432, CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: mysql55-mysql on SL5.x i386/x86_64 (1508-16594)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=16594

SL5
x86_64
mysql55-mysql-debuginfo-5.5.45-1.el5
mysql55-mysql-server-5.5.45-1.el5
mysql55-mysql-test-5.5.45-1.el5
mysql55-mysql-bench-5.5.45-1.el5
mysql55-mysql-5.5.45-1.el5
mysql55-mysql-devel-5.5.45-1.el5
mysql55-mysql-libs-5.5.45-1.el5

i386
mysql55-mysql-debuginfo-5.5.45-1.el5
mysql55-mysql-server-5.5.45-1.el5
mysql55-mysql-test-5.5.45-1.el5
mysql55-mysql-bench-5.5.45-1.el5
mysql55-mysql-5.5.45-1.el5
mysql55-mysql-devel-5.5.45-1.el5
mysql55-mysql-libs-5.5.45-1.el5

174790 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1507-12946)

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

Risk Level: High

CVE: CVE-2015-5477

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: bind97 on SL5.x i386/x86_64 (1507-12946)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=12946

SL5
x86_64
bind97-devel-9.7.0-21.P2.el5_11.2
bind97-chroot-9.7.0-21.P2.el5_11.2
bind97-libs-9.7.0-21.P2.el5_11.2
bind97-debuginfo-9.7.0-21.P2.el5_11.2
bind97-utils-9.7.0-21.P2.el5_11.2
bind97-9.7.0-21.P2.el5_11.2

i386
bind97-devel-9.7.0-21.P2.el5_11.2
bind97-chroot-9.7.0-21.P2.el5_11.2
bind97-libs-9.7.0-21.P2.el5_11.2
bind97-debuginfo-9.7.0-21.P2.el5_11.2
bind97-utils-9.7.0-21.P2.el5_11.2
bind97-9.7.0-21.P2.el5_11.2

174792 - Scientific Linux Security ERRATA Moderate: php on SL6.x i386/x86_64 (1507-6144)

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

Risk Level: High

CVE: CVE-2014-9425, CVE-2014-9705, CVE-2014-9709, CVE-2015-0232, CVE-2015-0273, CVE-2015-2301, CVE-2015-2783, CVE-2015-2787, CVE-2015-3307, CVE-2015-3329, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4598, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: php on SL6.x i386/x86_64 (1507-6144)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=6144

SL6
x86_64
php-recode-5.3.3-46.el6_6
php-imap-5.3.3-46.el6_6
php-xml-5.3.3-46.el6_6
php-zts-5.3.3-46.el6_6
php-mysql-5.3.3-46.el6_6
php-soap-5.3.3-46.el6_6
php-process-5.3.3-46.el6_6
php-cli-5.3.3-46.el6_6
php-mbstring-5.3.3-46.el6_6

php-dba-5.3.3-46.el6_6
php-tidy-5.3.3-46.el6_6
php-xmlrpc-5.3.3-46.el6_6
php-pdo-5.3.3-46.el6_6
php-devel-5.3.3-46.el6_6
php-bcmath-5.3.3-46.el6_6
php-fpm-5.3.3-46.el6_6
php-embedded-5.3.3-46.el6_6
php-intl-5.3.3-46.el6_6
php-pspell-5.3.3-46.el6_6
php-snmp-5.3.3-46.el6_6
php-debuginfo-5.3.3-46.el6_6
php-pgsql-5.3.3-46.el6_6
php-5.3.3-46.el6_6
php-ldap-5.3.3-46.el6_6
php-odbc-5.3.3-46.el6_6
php-gd-5.3.3-46.el6_6
php-common-5.3.3-46.el6_6
php-enchant-5.3.3-46.el6_6

i386
php-recode-5.3.3-46.el6_6
php-imap-5.3.3-46.el6_6
php-xml-5.3.3-46.el6_6
php-zts-5.3.3-46.el6_6
php-mysql-5.3.3-46.el6_6
php-soap-5.3.3-46.el6_6
php-process-5.3.3-46.el6_6
php-cli-5.3.3-46.el6_6
php-mbstring-5.3.3-46.el6_6
php-dba-5.3.3-46.el6_6
php-tidy-5.3.3-46.el6_6
php-xmlrpc-5.3.3-46.el6_6
php-pdo-5.3.3-46.el6_6
php-devel-5.3.3-46.el6_6
php-bcmath-5.3.3-46.el6_6
php-fpm-5.3.3-46.el6_6
php-embedded-5.3.3-46.el6_6
php-intl-5.3.3-46.el6_6
php-pspell-5.3.3-46.el6_6
php-snmp-5.3.3-46.el6_6
php-debuginfo-5.3.3-46.el6_6
php-pgsql-5.3.3-46.el6_6
php-5.3.3-46.el6_6
php-ldap-5.3.3-46.el6_6
php-odbc-5.3.3-46.el6_6
php-gd-5.3.3-46.el6_6
php-common-5.3.3-46.el6_6
php-enchant-5.3.3-46.el6_6

174795 - Scientific Linux Security ERRATA Important: apache-commons-collections on SL7.x (noarch) (1511-17483)

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: apache-commons-collections on SL7.x (noarch) (1511-17483)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=17483

SL7
noarch
apache-commons-collections-3.2.1-22.el7_2
apache-commons-collections-testframework-javadoc-3.2.1-22.el7_2
apache-commons-collections-testframework-3.2.1-22.el7_2
apache-commons-collections-javadoc-3.2.1-22.el7_2

174796 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-16660)

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7189, CVE-2015-7193, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86_64 (1511-16660)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=16660

SL5
x86_64
thunderbird-38.4.0-1.el5_11
thunderbird-debuginfo-38.4.0-1.el5_11

i386
thunderbird-38.4.0-1.el5_11
thunderbird-debuginfo-38.4.0-1.el5_11

SL7
x86_64
thunderbird-38.4.0-1.el7_2
thunderbird-debuginfo-38.4.0-1.el7_2

SL6
x86_64
thunderbird-debuginfo-38.4.0-1.el6_7
thunderbird-38.4.0-1.el6_7

i386
thunderbird-debuginfo-38.4.0-1.el6_7
thunderbird-38.4.0-1.el6_7

174803 - Scientific Linux Security ERRATA Moderate: python on SL6.x i386/x86_64 (1508-3564)

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

Risk Level: High

CVE: CVE-2013-1752, CVE-2014-1912, CVE-2014-4650, CVE-2014-7185

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: python on SL6.x i386/x86_64 (1508-3564)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=3564

SL6
x86_64
python-2.6.6-64.el6
tkinter-2.6.6-64.el6
python-debuginfo-2.6.6-64.el6
python-test-2.6.6-64.el6
python-libs-2.6.6-64.el6
python-tools-2.6.6-64.el6
python-devel-2.6.6-64.el6

i386
python-2.6.6-64.el6
tkinter-2.6.6-64.el6
python-debuginfo-2.6.6-64.el6
python-test-2.6.6-64.el6
python-libs-2.6.6-64.el6
python-tools-2.6.6-64.el6
python-devel-2.6.6-64.el6

174810 - Scientific Linux Security ERRATA Important: libuser on SL6.x i386/x86_64 (1508-403)

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

Risk Level: High

CVE: CVE-2015-3245, CVE-2015-3246

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libuser on SL6.x i386/x86_64 (1508-403)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=403

SL6
x86_64
libuser-devel-0.56.13-8.el6_7
libuser-debuginfo-0.56.13-8.el6_7
libuser-0.56.13-8.el6_7
libuser-python-0.56.13-8.el6_7

i386
libuser-devel-0.56.13-8.el6_7
libuser-debuginfo-0.56.13-8.el6_7

libuser-0.56.13-8.el6_7
libuser-python-0.56.13-8.el6_7

174811 - Scientific Linux Security ERRATA Important: php on SL7.x x86_64 (1506-12640)

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

Risk Level: High

CVE: CVE-2014-8142, CVE-2014-9652, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232, CVE-2015-0273, CVE-2015-2301, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3307, CVE-2015-3329, CVE-2015-3330, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4598, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: php on SL7.x x86_64 (1506-12640)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=12640

SL7
x86_64
php-mysql-5.4.16-36.el7_1
php-bcmath-5.4.16-36.el7_1
php-intl-5.4.16-36.el7_1
php-pgsql-5.4.16-36.el7_1
php-soap-5.4.16-36.el7_1
php-devel-5.4.16-36.el7_1
php-process-5.4.16-36.el7_1
php-common-5.4.16-36.el7_1
php-debuginfo-5.4.16-36.el7_1
php-mysqlnd-5.4.16-36.el7_1
php-cli-5.4.16-36.el7_1
php-xmlrpc-5.4.16-36.el7_1
php-odbc-5.4.16-36.el7_1
php-fpm-5.4.16-36.el7_1
php-recode-5.4.16-36.el7_1
php-snmp-5.4.16-36.el7_1
php-gd-5.4.16-36.el7_1
php-enchant-5.4.16-36.el7_1
php-5.4.16-36.el7_1
php-ldap-5.4.16-36.el7_1
php-pdo-5.4.16-36.el7_1
php-pspell-5.4.16-36.el7_1
php-mbstring-5.4.16-36.el7_1
php-embedded-5.4.16-36.el7_1
php-xml-5.4.16-36.el7_1
php-dba-5.4.16-36.el7_1

174812 - Scientific Linux Security ERRATA Moderate: sqlite on SL6.x i386/x86_64 (1508-15942)

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

Risk Level: High

CVE: CVE-2015-3416

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: sqlite on SL6.x i386/x86_64 (1508-15942)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=15942

SL6
x86_64
sqlite-tcl-3.6.20-1.el6_7.2
sqlite-devel-3.6.20-1.el6_7.2
sqlite-debuginfo-3.6.20-1.el6_7.2
sqlite-3.6.20-1.el6_7.2
lemon-3.6.20-1.el6_7.2
sqlite-doc-3.6.20-1.el6_7.2

i386
sqlite-tcl-3.6.20-1.el6_7.2
sqlite-devel-3.6.20-1.el6_7.2
sqlite-debuginfo-3.6.20-1.el6_7.2
sqlite-3.6.20-1.el6_7.2
lemon-3.6.20-1.el6_7.2
sqlite-doc-3.6.20-1.el6_7.2

174816 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1510-4832)

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

Risk Level: High

CVE: CVE-2015-5279

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1510-4832)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=4832

SL6
x86_64
qemu-img-0.12.1.2-2.479.el6_7.2
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.2
qemu-guest-agent-0.12.1.2-2.479.el6_7.2
qemu-kvm-0.12.1.2-2.479.el6_7.2
qemu-kvm-tools-0.12.1.2-2.479.el6_7.2

i386
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.2
qemu-guest-agent-0.12.1.2-2.479.el6_7.2

174817 - Scientific Linux Security ERRATA Moderate: mailman on SL7.x x86_64 (1506-13904)

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

Risk Level: High

CVE: CVE-2015-2775

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: mailman on SL7.x x86_64 (1506-13904)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=13904

SL7
x86_64
mailman-debuginfo-2.1.15-21.el7_1
mailman-2.1.15-21.el7_1

174820 - Scientific Linux Security ERRATA Important: libuser on SL7.x x86_64 (1507-10651)

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

Risk Level: High

CVE: CVE-2015-3245, CVE-2015-3246

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libuser on SL7.x x86_64 (1507-10651)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=10651

SL7
x86_64
libuser-python-0.60-7.el7_1
libuser-devel-0.60-7.el7_1
libuser-0.60-7.el7_1
libuser-debuginfo-0.60-7.el7_1

174825 - Scientific Linux Security ERRATA Moderate: clutter on SL7.x x86_64 (1507-12620)

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

Risk Level: High

CVE: CVE-2015-3213

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: clutter on SL7.x x86_64 (1507-12620)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=12620

SL7
x86_64
clutter-1.14.4-12.el7_1.1
clutter-debuginfo-1.14.4-12.el7_1.1
clutter-devel-1.14.4-12.el7_1.1
clutter-doc-1.14.4-12.el7_1.1

174827 - Scientific Linux Security ERRATA Important: kvm on SL5.x x86_64 (1510-4514)

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

Risk Level: High

CVE: CVE-2015-5279

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kvm on SL5.x x86_64 (1510-4514)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=4514

SL5
x86_64
kvm-83-274.el5_11
kvm-tools-83-274.el5_11
kmod-kvm-83-274.el5_11
kmod-kvm-debug-83-274.el5_11
kvm-qemu-img-83-274.el5_11
kvm-debuginfo-83-274.el5_11

174830 - Scientific Linux Security ERRATA Important: jakarta-commons-collections on SL6.x (noarch) (1511-17116)

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

Risk Level: High

CVE: CVE-2015-7501

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: jakarta-commons-collections on SL6.x (noarch) (1511-17116)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=17116

SL6
noarch
jakarta-commons-collections-testframework-javadoc-3.2.1-3.5.el6_7

jakarta-commons-collections-3.2.1-3.5.el6_7
jakarta-commons-collections-testframework-3.2.1-3.5.el6_7
jakarta-commons-collections-tomcat5-3.2.1-3.5.el6_7
jakarta-commons-collections-javadoc-3.2.1-3.5.el6_7

178070 - Gentoo Linux GLSA-201506-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1233, CVE-2015-1234, CVE-2015-1235, CVE-2015-1236, CVE-2015-1237, CVE-2015-1238, CVE-2015-1240, CVE-2015-1241, CVE-2015-1242, CVE-2015-1243, CVE-2015-1244, CVE-2015-1245, CVE-2015-1246, CVE-2015-1247, CVE-2015-1248, CVE-2015-1250, CVE-2015-1251, CVE-2015-1252, CVE-2015-1253, CVE-2015-1254, CVE-2015-1255, CVE-2015-1256, CVE-2015-1257, CVE-2015-1258, CVE-2015-1259, CVE-2015-1260, CVE-2015-1262, CVE-2015-1263, CVE-2015-1264, CVE-2015-1265

Description

The scan detected that the host is missing the following update:
GLSA-201506-04

Observation

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

https://security.gentoo.org/glsa/201506-04

Affected packages:
www-client/chromium < 43.0.2357.65

178074 - Gentoo Linux GLSA-201507-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3414, CVE-2015-3415, CVE-2015-3416

Description

The scan detected that the host is missing the following update:
GLSA-201507-05

Observation

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

https://security.gentoo.org/glsa/201507-05

Affected packages:
dev-db/sqlite < 3.8.9

178078 - Gentoo Linux GLSA-201507-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147

Description

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

GLSA-201507-04

Observation

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

https://security.gentoo.org/glsa/201507-04

Affected packages:
dev-libs/icu < 55.1

178080 - Gentoo Linux GLSA-201507-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3905

Description

The scan detected that the host is missing the following update:
GLSA-201507-10

Observation

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

https://security.gentoo.org/glsa/201507-10

Affected packages:
app-text/t1utils < 1.39

178081 - Gentoo Linux GLSA-201504-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6568, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0385, CVE-2015-0391, CVE-2015-0409, CVE-2015-0411, CVE-2015-0432

Description

The scan detected that the host is missing the following update:
GLSA-201504-05

Observation

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

https://security.gentoo.org/glsa/201504-05

Affected packages:
dev-db/mysql < 5.6.22
dev-db/mariadb < 10.0.16

178083 - Gentoo Linux GLSA-201510-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3258, CVE-2015-3279

Description

The scan detected that the host is missing the following update:
GLSA-201510-08

Observation

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

https://security.gentoo.org/glsa/201510-08

Affected packages:
net-print/cups-filters < 1.0.71

178084 - Gentoo Linux GLSA-201506-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3308

Description

The scan detected that the host is missing the following update:
GLSA-201506-03

Observation

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

https://security.gentoo.org/glsa/201506-03

Affected packages:
net-libs/gnutls < 3.3.15

178085 - Gentoo Linux GLSA-201507-11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7422

Description

The scan detected that the host is missing the following update:
GLSA-201507-11

Observation

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

https://security.gentoo.org/glsa/201507-11

Affected packages:
dev-lang/perl < 5.20.1-r4

178097 - Gentoo Linux GLSA-201503-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7923, CVE-2014-7926, CVE-2014-7940, CVE-2014-9654

Description

The scan detected that the host is missing the following update:
GLSA-201503-06

Observation

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

https://security.gentoo.org/glsa/201503-06

Affected packages:
dev-libs/icu < 54.1-r1

178099 - Gentoo Linux GLSA-201510-05 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2931, CVE-2015-2932, CVE-2015-2933, CVE-2015-2934, CVE-2015-2935, CVE-2015-2936, CVE-2015-2937, CVE-2015-2938, CVE-2015-2939, CVE-2015-2940, CVE-2015-2941, CVE-2015-2942, CVE-2015-6728, CVE-2015-6729, CVE-2015-6730, CVE-2015-6731, CVE-2015-6732, CVE-2015-6733, CVE-2015-6734, CVE-2015-6735, CVE-2015-6736, CVE-2015-6737

Description

The scan detected that the host is missing the following update:
GLSA-201510-05

Observation

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

https://security.gentoo.org/glsa/201510-05

Affected packages:
www-apps/mediawiki < 1.25.2

178100 - Gentoo Linux GLSA-201509-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2326, CVE-2014-2327, CVE-2014-2328, CVE-2014-2708, CVE-2014-2709, CVE-2014-4002, CVE-2014-5025, CVE-2014-5026, CVE-2015-2967

Description

The scan detected that the host is missing the following update:
GLSA-201509-03

Observation

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

https://security.gentoo.org/glsa/201509-03

Affected packages:
net-analyzer/cacti < 0.8.8d

178101 - Gentoo Linux GLSA-201510-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5143, CVE-2015-5144, CVE-2015-5145

Description

The scan detected that the host is missing the following update:
GLSA-201510-06

Observation

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

https://security.gentoo.org/glsa/201510-06

Affected packages:
dev-python/django < 1.8.3

178104 - Gentoo Linux GLSA-201503-12 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1213, CVE-2015-1214, CVE-2015-1215, CVE-2015-1216, CVE-2015-1217, CVE-2015-1218, CVE-2015-1219, CVE-2015-1220, CVE-2015-1221, CVE-2015-1222, CVE-2015-1223, CVE-2015-1224, CVE-2015-1225, CVE-2015-1226, CVE-2015-1227, CVE-2015-1228, CVE-2015-1229, CVE-2015-1230, CVE-2015-1231, CVE-2015-1232

Description

The scan detected that the host is missing the following update:
GLSA-201503-12

Observation

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

https://security.gentoo.org/glsa/201503-12

Affected packages:
www-client/chromium < 41.0.2272.76

178106 - Gentoo Linux GLSA-201507-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1502

Description

The scan detected that the host is missing the following update:
GLSA-201507-09

Observation

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

https://security.gentoo.org/glsa/201507-09

Affected packages:
dev-python/pypam < 0.5.0-r3

178109 - Gentoo Linux GLSA-201503-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1752, CVE-2013-7338, CVE-2014-1912, CVE-2014-2667, CVE-2014-4616, CVE-2014-7185, CVE-2014-9365

Description

The scan detected that the host is missing the following update:
GLSA-201503-10

Observation

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

https://security.gentoo.org/glsa/201503-10

Affected packages:
dev-lang/python < 3.3.5-r1

178111 - Gentoo Linux GLSA-201510-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1349, CVE-2015-4620, CVE-2015-5477, CVE-2015-5722, CVE-2015-5986

Description

The scan detected that the host is missing the following update:
GLSA-201510-01

Observation

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

https://security.gentoo.org/glsa/201510-01

Affected packages:
net-dns/bind < 9.10.2_p4

178112 - Gentoo Linux GLSA-201503-11 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0204, CVE-2015-0207, CVE-2015-0208, CVE-2015-0209, CVE-2015-0285, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0290, CVE-2015-0291, CVE-2015-0292, CVE-2015-0293, CVE-2015-1787

Description

The scan detected that the host is missing the following update:
GLSA-201503-11

Observation

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

https://security.gentoo.org/glsa/201503-11

Affected packages:
dev-libs/openssl < 1.0.1l-r1

178113 - Gentoo Linux GLSA-201510-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3209, CVE-2015-3214, CVE-2015-5154, CVE-2015-5158

Description

The scan detected that the host is missing the following update:
GLSA-201510-02

Observation

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

https://security.gentoo.org/glsa/201510-02

Affected packages:
app-emulation/qemu < 2.3.0-r4

178114 - Gentoo Linux GLSA-201510-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2187, CVE-2015-2188, CVE-2015-2189, CVE-2015-2190, CVE-2015-2191, CVE-2015-2192, CVE-2015-3182, CVE-2015-3808, CVE-2015-3809, CVE-2015-3810, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813, CVE-2015-3814, CVE-2015-3815, CVE-2015-3906, CVE-2015-4651, CVE-2015-4652

Description

The scan detected that the host is missing the following update:
GLSA-201510-03

Observation

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

https://security.gentoo.org/glsa/201510-03

Affected packages:
net-analyzer/wireshark < 1.12.7

178115 - Gentoo Linux GLSA-201507-07 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-6052, CVE-2014-6053, CVE-2014-6054, CVE-2014-6055

Description

The scan detected that the host is missing the following update:
GLSA-201507-07

Observation

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

https://security.gentoo.org/glsa/201507-07

Affected packages:
net-libs/libvncserver < 0.9.10-r1

178116 - Gentoo Linux GLSA-201510-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155

Description

The scan detected that the host is missing the following update:
GLSA-201510-04

Observation

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

https://security.gentoo.org/glsa/201510-04

Affected packages:
net-analyzer/tcpdump < 4.7.4

178121 - Gentoo Linux GLSA-201504-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2212, CVE-2013-3495, CVE-2014-3967, CVE-2014-3968, CVE-2014-5146, CVE-2014-5149, CVE-2014-8594, CVE-2014-8595, CVE-2014-8866, CVE-2014-8867, CVE-2014-9030, CVE-2014-9065, CVE-2014-9066, CVE-2015-0361, CVE-2015-2044, CVE-2015-2045, CVE-2015-2152, CVE-2015-2751, CVE-2015-2752, CVE-2015-2756

Description

The scan detected that the host is missing the following update:
GLSA-201504-04

Observation

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

https://security.gentoo.org/glsa/201504-04

Affected packages:
app-emulation/xen < 4.4.2-r1

178125 - Gentoo Linux GLSA-201508-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4488, CVE-2013-6487, CVE-2014-3775

Description

The scan detected that the host is missing the following update:
GLSA-201508-02

Observation

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

https://security.gentoo.org/glsa/201508-02

Affected packages:
net-libs/libgadu < 1.12.0

178129 - Gentoo Linux GLSA-201507-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9274, CVE-2014-9275

Description

The scan detected that the host is missing the following update:
GLSA-201507-06

Observation

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

https://security.gentoo.org/glsa/201507-06

Affected packages:
app-text/unrtf < 0.21.9

178132 - Gentoo Linux GLSA-201506-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8176, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-4000

Description

The scan detected that the host is missing the following update:
GLSA-201506-02

Observation

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

https://security.gentoo.org/glsa/201506-02

Affected packages:
dev-libs/openssl < 1.0.1o

178133 - Gentoo Linux GLSA-201505-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6395, CVE-2014-6396, CVE-2014-9376, CVE-2014-9377, CVE-2014-9378, CVE-2014-9379, CVE-2014-9380, CVE-2014-9381

Description

The scan detected that the host is missing the following update:
GLSA-201505-01

Observation

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

https://security.gentoo.org/glsa/201505-01

Affected packages:
net-analyzer/ettercap < 0.8.2

190099 - Fedora Linux 22 FEDORA-2015-afafa29551 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8380

Description

The scan detected that the host is missing the following update:
FEDORA-2015-afafa29551

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173700.html

Fedora Core 22

pcre-8.37-7.fc22

91975 - Oracle Enterprise Linux ELSA-2015-2636 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-7613, CVE-2015-7872, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
ELSA-2015-2636

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005638.html

OEL6
x86_64
perf-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

i386
perf-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

91977 - Oracle Enterprise Linux ELSA-2015-2619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
ELSA-2015-2619

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005629.html
http://oss.oracle.com/pipermail/el-errata/2015-December/005626.html

OEL7
x86_64
libreoffice-langpack-pa-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ja-4.3.7.2-5.0.1.el7_2.1
libreoffice-bsh-4.3.7.2-5.0.1.el7_2.1

libreoffice-langpack-nb-4.3.7.2-5.0.1.el7_2.1
libreoffice-wiki-publisher-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ss-4.3.7.2-5.0.1.el7_2.1
libreoffice-sdk-doc-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ts-4.3.7.2-5.0.1.el7_2.1
autocorr-tr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-en-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-sl-4.3.7.2-5.0.1.el7_2.1
autocorr-pl-4.3.7.2-5.0.1.el7_2.1
autocorr-ko-4.3.7.2-5.0.1.el7_2.1
autocorr-ro-4.3.7.2-5.0.1.el7_2.1
libreoffice-headless-4.3.7.2-5.0.1.el7_2.1
autocorr-it-4.3.7.2-5.0.1.el7_2.1
libreoffice-rhino-4.3.7.2-5.0.1.el7_2.1
autocorr-ga-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-el-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-bg-4.3.7.2-5.0.1.el7_2.1
libreoffice-writer-4.3.7.2-5.0.1.el7_2.1
autocorr-lt-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-pt-PT-4.3.7.2-5.0.1.el7_2.1
autocorr-vi-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ro-4.3.7.2-5.0.1.el7_2.1
libreoffice-ure-4.3.7.2-5.0.1.el7_2.1
autocorr-hu-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-kk-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-pt-BR-4.3.7.2-5.0.1.el7_2.1
libreoffice-librelogo-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-st-4.3.7.2-5.0.1.el7_2.1
autocorr-bg-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ml-4.3.7.2-5.0.1.el7_2.1
autocorr-en-4.3.7.2-5.0.1.el7_2.1
autocorr-sl-4.3.7.2-5.0.1.el7_2.1
libreoffice-draw-4.3.7.2-5.0.1.el7_2.1
autocorr-pt-4.3.7.2-5.0.1.el7_2.1
libreoffice-nlpsolver-4.3.7.2-5.0.1.el7_2.1
autocorr-sk-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-sr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-kn-4.3.7.2-5.0.1.el7_2.1
autocorr-es-4.3.7.2-5.0.1.el7_2.1
libreoffice-math-4.3.7.2-5.0.1.el7_2.1
autocorr-ru-4.3.7.2-5.0.1.el7_2.1
libreoffice-pdfimport-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-dz-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-hu-4.3.7.2-5.0.1.el7_2.1
autocorr-nl-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ca-4.3.7.2-5.0.1.el7_2.1
autocorr-sv-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-or-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-uk-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-hi-4.3.7.2-5.0.1.el7_2.1
autocorr-is-4.3.7.2-5.0.1.el7_2.1
libreoffice-pyuno-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-he-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-mai-4.3.7.2-5.0.1.el7_2.1
libreoffice-sdk-4.3.7.2-5.0.1.el7_2.1
libreoffice-base-4.3.7.2-5.0.1.el7_2.1
autocorr-fi-4.3.7.2-5.0.1.el7_2.1
autocorr-ca-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-tr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-nr-4.3.7.2-5.0.1.el7_2.1

libreoffice-langpack-ga-4.3.7.2-5.0.1.el7_2.1
autocorr-ja-4.3.7.2-5.0.1.el7_2.1
libreoffice-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-zu-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-es-4.3.7.2-5.0.1.el7_2.1
autocorr-lb-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-nn-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-br-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ta-4.3.7.2-5.0.1.el7_2.1
libreoffice-ogltrans-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-cs-4.3.7.2-5.0.1.el7_2.1
autocorr-sr-4.3.7.2-5.0.1.el7_2.1
autocorr-fa-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-fa-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-gl-4.3.7.2-5.0.1.el7_2.1
libreoffice-filters-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-nl-4.3.7.2-5.0.1.el7_2.1
libreoffice-core-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-nso-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-pl-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-hr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-da-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-th-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-bn-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-it-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-zh-Hant-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ve-4.3.7.2-5.0.1.el7_2.1
libreoffice-calc-4.3.7.2-5.0.1.el7_2.1
libreoffice-xsltfilter-4.3.7.2-5.0.1.el7_2.1
libreoffice-impress-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-si-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-eu-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ru-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-sv-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-lv-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-af-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-et-4.3.7.2-5.0.1.el7_2.1
libreoffice-opensymbol-fonts-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-tn-4.3.7.2-5.0.1.el7_2.1
autocorr-hr-4.3.7.2-5.0.1.el7_2.1
autocorr-de-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ko-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-lt-4.3.7.2-5.0.1.el7_2.1
autocorr-mn-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-mr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-xh-4.3.7.2-5.0.1.el7_2.1
autocorr-af-4.3.7.2-5.0.1.el7_2.1
libreoffice-emailmerge-4.3.7.2-5.0.1.el7_2.1
libreoffice-glade-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-de-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-zh-Hans-4.3.7.2-5.0.1.el7_2.1
libreoffice-postgresql-4.3.7.2-5.0.1.el7_2.1
libreoffice-graphicfilter-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-ar-4.3.7.2-5.0.1.el7_2.1
autocorr-fr-4.3.7.2-5.0.1.el7_2.1
libreoffice-officebean-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-sk-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-fi-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-gu-4.3.7.2-5.0.1.el7_2.1
autocorr-cs-4.3.7.2-5.0.1.el7_2.1

libreoffice-langpack-as-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-fr-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-cy-4.3.7.2-5.0.1.el7_2.1
autocorr-da-4.3.7.2-5.0.1.el7_2.1
autocorr-zh-4.3.7.2-5.0.1.el7_2.1
libreoffice-gdb-debug-support-4.3.7.2-5.0.1.el7_2.1
libreoffice-langpack-te-4.3.7.2-5.0.1.el7_2.1

OEL6
x86_64
autocorr-es-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-ss-4.2.8.2-11.0.1.el6_7.1
autocorr-zh-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-bn-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.0.1.el6_7.1
autocorr-nl-4.2.8.2-11.0.1.el6_7.1
libreoffice-xsltfilter-4.2.8.2-11.0.1.el6_7.1
autocorr-sl-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.0.1.el6_7.1
libreoffice-wiki-publisher-4.2.8.2-11.0.1.el6_7.1
autocorr-is-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-sr-4.2.8.2-11.0.1.el6_7.1
autocorr-hr-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.0.1.el6_7.1
autocorr-ca-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-et-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-gu-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-mai-4.2.8.2-11.0.1.el6_7.1
autocorr-lt-4.2.8.2-11.0.1.el6_7.1
libreoffice-4.2.8.2-11.0.1.el6_7.1
libreoffice-glade-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-pt-BR-4.2.8.2-11.0.1.el6_7.1
autocorr-hu-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.0.1.el6_7.1
libreoffice-pdfimport-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-nn-4.2.8.2-11.0.1.el6_7.1
autocorr-cs-4.2.8.2-11.0.1.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.0.1.el6_7.1

130335 - Debian Linux 8.0 DSA-3414-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3259, CVE-2015-3340, CVE-2015-5307, CVE-2015-6654, CVE-2015-7311, CVE-2015-7812, CVE-2015-7813, CVE-2015-7814, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
DSA-3414-1

Observation

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

http://www.debian.org/security/2015/dsa-3414

Debian 8.0
all
libxen-4.4_4.4.1-9+deb8u3
xen-hypervisor-4.4-armhf_4.4.1-9+deb8u3
libxenstore3.0_4.4.1-9+deb8u3
xen-utils-4.4_4.4.1-9+deb8u3
xen-system-arm64_4.4.1-9+deb8u3
xen-hypervisor-4.4-amd64_4.4.1-9+deb8u3
xen-system-armhf_4.4.1-9+deb8u3
libxen-dev_4.4.1-9+deb8u3
xen-utils-common_4.4.1-9+deb8u3
xen-hypervisor-4.4-arm64_4.4.1-9+deb8u3
xen-system-amd64_4.4.1-9+deb8u3
xenstore-utils_4.4.1-9+deb8u3

141036 - Red Hat Enterprise Linux RHSA-2015-2619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
RHSA-2015-2619

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2619.html

RHEL6S
i386
libreoffice-math-4.2.8.2-11.el6_7.1
libreoffice-langpack-tr-4.2.8.2-11.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.el6_7.1
libreoffice-langpack-ga-4.2.8.2-11.el6_7.1
libreoffice-langpack-sv-4.2.8.2-11.el6_7.1
libreoffice-langpack-fi-4.2.8.2-11.el6_7.1
libreoffice-headless-4.2.8.2-11.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.el6_7.1
libreoffice-langpack-pl-4.2.8.2-11.el6_7.1
libreoffice-filters-4.2.8.2-11.el6_7.1
libreoffice-langpack-kn-4.2.8.2-11.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.el6_7.1
libreoffice-langpack-lt-4.2.8.2-11.el6_7.1
libreoffice-draw-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hant-4.2.8.2-11.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.el6_7.1
libreoffice-langpack-or-4.2.8.2-11.el6_7.1
libreoffice-langpack-mai-4.2.8.2-11.el6_7.1
libreoffice-langpack-hu-4.2.8.2-11.el6_7.1
libreoffice-langpack-nr-4.2.8.2-11.el6_7.1
libreoffice-pyuno-4.2.8.2-11.el6_7.1
libreoffice-ure-4.2.8.2-11.el6_7.1
libreoffice-langpack-nl-4.2.8.2-11.el6_7.1
libreoffice-langpack-ca-4.2.8.2-11.el6_7.1

libreoffice-langpack-ro-4.2.8.2-11.el6_7.1
libreoffice-langpack-zu-4.2.8.2-11.el6_7.1
libreoffice-debuginfo-4.2.8.2-11.el6_7.1
libreoffice-emailmerge-4.2.8.2-11.el6_7.1
libreoffice-glade-4.2.8.2-11.el6_7.1
libreoffice-langpack-bg-4.2.8.2-11.el6_7.1
libreoffice-librelogo-4.2.8.2-11.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.el6_7.1
libreoffice-langpack-ru-4.2.8.2-11.el6_7.1
libreoffice-langpack-da-4.2.8.2-11.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.el6_7.1
libreoffice-sdk-4.2.8.2-11.el6_7.1
libreoffice-langpack-as-4.2.8.2-11.el6_7.1
libreoffice-langpack-ta-4.2.8.2-11.el6_7.1
libreoffice-langpack-ur-4.2.8.2-11.el6_7.1
libreoffice-langpack-ve-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-PT-4.2.8.2-11.el6_7.1
libreoffice-base-4.2.8.2-11.el6_7.1
libreoffice-core-4.2.8.2-11.el6_7.1
libreoffice-langpack-pa-4.2.8.2-11.el6_7.1
libreoffice-sdk-doc-4.2.8.2-11.el6_7.1
libreoffice-langpack-cs-4.2.8.2-11.el6_7.1
libreoffice-rhino-4.2.8.2-11.el6_7.1
libreoffice-gdb-debug-support-4.2.8.2-11.el6_7.1
libreoffice-langpack-ss-4.2.8.2-11.el6_7.1
libreoffice-langpack-bn-4.2.8.2-11.el6_7.1
libreoffice-langpack-hi-4.2.8.2-11.el6_7.1
libreoffice-langpack-ar-4.2.8.2-11.el6_7.1
libreoffice-langpack-xh-4.2.8.2-11.el6_7.1
libreoffice-impress-4.2.8.2-11.el6_7.1
libreoffice-ogltrans-4.2.8.2-11.el6_7.1
libreoffice-xsltfilter-4.2.8.2-11.el6_7.1
libreoffice-graphicfilter-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hans-4.2.8.2-11.el6_7.1
libreoffice-wiki-publisher-4.2.8.2-11.el6_7.1
libreoffice-langpack-ts-4.2.8.2-11.el6_7.1
libreoffice-langpack-tn-4.2.8.2-11.el6_7.1
libreoffice-calc-4.2.8.2-11.el6_7.1
libreoffice-langpack-nb-4.2.8.2-11.el6_7.1
libreoffice-langpack-nso-4.2.8.2-11.el6_7.1
libreoffice-langpack-sl-4.2.8.2-11.el6_7.1
libreoffice-nlpsolver-4.2.8.2-11.el6_7.1
libreoffice-langpack-de-4.2.8.2-11.el6_7.1
libreoffice-langpack-dz-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-BR-4.2.8.2-11.el6_7.1
libreoffice-writer-4.2.8.2-11.el6_7.1
libreoffice-langpack-te-4.2.8.2-11.el6_7.1
libreoffice-langpack-et-4.2.8.2-11.el6_7.1
libreoffice-langpack-eu-4.2.8.2-11.el6_7.1
libreoffice-bsh-4.2.8.2-11.el6_7.1
libreoffice-langpack-cy-4.2.8.2-11.el6_7.1
libreoffice-langpack-hr-4.2.8.2-11.el6_7.1
libreoffice-langpack-nn-4.2.8.2-11.el6_7.1
libreoffice-4.2.8.2-11.el6_7.1
libreoffice-langpack-he-4.2.8.2-11.el6_7.1
libreoffice-langpack-sr-4.2.8.2-11.el6_7.1
libreoffice-langpack-en-4.2.8.2-11.el6_7.1
libreoffice-langpack-ml-4.2.8.2-11.el6_7.1
libreoffice-langpack-it-4.2.8.2-11.el6_7.1

libreoffice-langpack-gu-4.2.8.2-11.el6_7.1
libreoffice-langpack-mr-4.2.8.2-11.el6_7.1
libreoffice-langpack-th-4.2.8.2-11.el6_7.1
libreoffice-langpack-ms-4.2.8.2-11.el6_7.1
libreoffice-pdfimport-4.2.8.2-11.el6_7.1
libreoffice-langpack-ko-4.2.8.2-11.el6_7.1
libreoffice-langpack-st-4.2.8.2-11.el6_7.1

noarch
autocorr-cs-4.2.8.2-11.el6_7.1
autocorr-en-4.2.8.2-11.el6_7.1
autocorr-is-4.2.8.2-11.el6_7.1
autocorr-ja-4.2.8.2-11.el6_7.1
autocorr-sk-4.2.8.2-11.el6_7.1
autocorr-vi-4.2.8.2-11.el6_7.1
autocorr-af-4.2.8.2-11.el6_7.1
autocorr-da-4.2.8.2-11.el6_7.1
autocorr-es-4.2.8.2-11.el6_7.1
autocorr-fa-4.2.8.2-11.el6_7.1
libreoffice-opensymbol-fonts-4.2.8.2-11.el6_7.1
autocorr-lt-4.2.8.2-11.el6_7.1
autocorr-it-4.2.8.2-11.el6_7.1
autocorr-sl-4.2.8.2-11.el6_7.1
autocorr-ro-4.2.8.2-11.el6_7.1
autocorr-hu-4.2.8.2-11.el6_7.1
autocorr-tr-4.2.8.2-11.el6_7.1
autocorr-fi-4.2.8.2-11.el6_7.1
autocorr-ko-4.2.8.2-11.el6_7.1
autocorr-mn-4.2.8.2-11.el6_7.1
autocorr-bg-4.2.8.2-11.el6_7.1
autocorr-ga-4.2.8.2-11.el6_7.1
autocorr-pt-4.2.8.2-11.el6_7.1
autocorr-sr-4.2.8.2-11.el6_7.1
autocorr-ca-4.2.8.2-11.el6_7.1
autocorr-ru-4.2.8.2-11.el6_7.1
autocorr-hr-4.2.8.2-11.el6_7.1
autocorr-lb-4.2.8.2-11.el6_7.1
autocorr-nl-4.2.8.2-11.el6_7.1
autocorr-de-4.2.8.2-11.el6_7.1
autocorr-zh-4.2.8.2-11.el6_7.1
autocorr-sv-4.2.8.2-11.el6_7.1
autocorr-pl-4.2.8.2-11.el6_7.1
autocorr-fr-4.2.8.2-11.el6_7.1

x86_64
libreoffice-math-4.2.8.2-11.el6_7.1
libreoffice-langpack-tr-4.2.8.2-11.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.el6_7.1
libreoffice-langpack-ga-4.2.8.2-11.el6_7.1
libreoffice-langpack-sv-4.2.8.2-11.el6_7.1
libreoffice-langpack-fi-4.2.8.2-11.el6_7.1
libreoffice-headless-4.2.8.2-11.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.el6_7.1
libreoffice-langpack-pl-4.2.8.2-11.el6_7.1
libreoffice-filters-4.2.8.2-11.el6_7.1
libreoffice-langpack-kn-4.2.8.2-11.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.el6_7.1
libreoffice-langpack-lt-4.2.8.2-11.el6_7.1
libreoffice-draw-4.2.8.2-11.el6_7.1

libreoffice-langpack-zh-Hant-4.2.8.2-11.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.el6_7.1
libreoffice-langpack-or-4.2.8.2-11.el6_7.1
libreoffice-langpack-mai-4.2.8.2-11.el6_7.1
libreoffice-langpack-hu-4.2.8.2-11.el6_7.1
libreoffice-langpack-nr-4.2.8.2-11.el6_7.1
libreoffice-pyuno-4.2.8.2-11.el6_7.1
libreoffice-ure-4.2.8.2-11.el6_7.1
libreoffice-langpack-nl-4.2.8.2-11.el6_7.1
libreoffice-langpack-ca-4.2.8.2-11.el6_7.1
libreoffice-langpack-ro-4.2.8.2-11.el6_7.1
libreoffice-langpack-zu-4.2.8.2-11.el6_7.1
libreoffice-debuginfo-4.2.8.2-11.el6_7.1
libreoffice-emailmerge-4.2.8.2-11.el6_7.1
libreoffice-glade-4.2.8.2-11.el6_7.1
libreoffice-langpack-bg-4.2.8.2-11.el6_7.1
libreoffice-librelogo-4.2.8.2-11.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.el6_7.1
libreoffice-langpack-ru-4.2.8.2-11.el6_7.1
libreoffice-langpack-da-4.2.8.2-11.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.el6_7.1
libreoffice-sdk-4.2.8.2-11.el6_7.1
libreoffice-langpack-as-4.2.8.2-11.el6_7.1
libreoffice-langpack-ta-4.2.8.2-11.el6_7.1
libreoffice-langpack-ur-4.2.8.2-11.el6_7.1
libreoffice-langpack-ve-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-PT-4.2.8.2-11.el6_7.1
libreoffice-base-4.2.8.2-11.el6_7.1
libreoffice-core-4.2.8.2-11.el6_7.1

RHEL6WS
i386
libreoffice-math-4.2.8.2-11.el6_7.1

RHEL7D
x86_64
libreoffice-langpack-ts-4.3.7.2-5.el7_2.1

RHEL6D
i386
libreoffice-math-4.2.8.2-11.el6_7.1

RHEL7WS
x86_64
libreoffice-langpack-ts-4.3.7.2-5.el7_2.1

141040 - Red Hat Enterprise Linux RHSA-2015-2636 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-7613, CVE-2015-7872, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
RHSA-2015-2636

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2636.html

RHEL6D
i386
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6

x86_64
perf-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6

RHEL6S
i386
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6

x86_64
perf-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6

RHEL6WS
i386
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6

x86_64
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6

160011 - CentOS 6 CESA-2015-2636 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-7613, CVE-2015-7872, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
CESA-2015-2636

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021541.html

CentOS 6
i686
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6

x86_64
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

160012 - CentOS 6, 7 CESA-2015-2619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
CESA-2015-2619

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021522.html
http://lists.centos.org/pipermail/centos-announce/2015-December/021521.html

CentOS 7
x86_64
libreoffice-langpack-sr-4.3.7.2-5.el7_2.1
libreoffice-langpack-ts-4.3.7.2-5.el7_2.1
libreoffice-officebean-4.3.7.2-5.el7_2.1
libreoffice-langpack-th-4.3.7.2-5.el7_2.1
libreoffice-langpack-lv-4.3.7.2-5.el7_2.1
libreoffice-glade-4.3.7.2-5.el7_2.1
libreoffice-math-4.3.7.2-5.el7_2.1
libreoffice-calc-4.3.7.2-5.el7_2.1
libreoffice-langpack-gu-4.3.7.2-5.el7_2.1

libreoffice-langpack-el-4.3.7.2-5.el7_2.1
libreoffice-langpack-nl-4.3.7.2-5.el7_2.1
libreoffice-langpack-ru-4.3.7.2-5.el7_2.1
libreoffice-langpack-as-4.3.7.2-5.el7_2.1
libreoffice-langpack-br-4.3.7.2-5.el7_2.1
libreoffice-xsltfilter-4.3.7.2-5.el7_2.1
libreoffice-pdfimport-4.3.7.2-5.el7_2.1
libreoffice-langpack-de-4.3.7.2-5.el7_2.1
libreoffice-langpack-zh-Hans-4.3.7.2-5.el7_2.1
libreoffice-langpack-it-4.3.7.2-5.el7_2.1
libreoffice-langpack-tn-4.3.7.2-5.el7_2.1
libreoffice-4.3.7.2-5.el7_2.1
libreoffice-nlpsolver-4.3.7.2-5.el7_2.1
libreoffice-langpack-eu-4.3.7.2-5.el7_2.1
libreoffice-gdb-debug-support-4.3.7.2-5.el7_2.1
libreoffice-langpack-ss-4.3.7.2-5.el7_2.1
libreoffice-writer-4.3.7.2-5.el7_2.1
libreoffice-ure-4.3.7.2-5.el7_2.1
libreoffice-langpack-ta-4.3.7.2-5.el7_2.1
libreoffice-sdk-4.3.7.2-5.el7_2.1
libreoffice-langpack-nb-4.3.7.2-5.el7_2.1
libreoffice-headless-4.3.7.2-5.el7_2.1
libreoffice-langpack-te-4.3.7.2-5.el7_2.1
libreoffice-langpack-kn-4.3.7.2-5.el7_2.1
libreoffice-langpack-pa-4.3.7.2-5.el7_2.1
libreoffice-langpack-sv-4.3.7.2-5.el7_2.1
libreoffice-core-4.3.7.2-5.el7_2.1
libreoffice-langpack-pl-4.3.7.2-5.el7_2.1
libreoffice-rhino-4.3.7.2-5.el7_2.1
libreoffice-langpack-cy-4.3.7.2-5.el7_2.1
libreoffice-sdk-doc-4.3.7.2-5.el7_2.1
libreoffice-langpack-nr-4.3.7.2-5.el7_2.1
libreoffice-langpack-pt-BR-4.3.7.2-5.el7_2.1
libreoffice-langpack-dz-4.3.7.2-5.el7_2.1
libreoffice-langpack-da-4.3.7.2-5.el7_2.1
libreoffice-langpack-ml-4.3.7.2-5.el7_2.1
libreoffice-langpack-gl-4.3.7.2-5.el7_2.1
libreoffice-langpack-ar-4.3.7.2-5.el7_2.1
libreoffice-langpack-ve-4.3.7.2-5.el7_2.1
libreoffice-langpack-mai-4.3.7.2-5.el7_2.1
libreoffice-langpack-st-4.3.7.2-5.el7_2.1
libreoffice-langpack-sl-4.3.7.2-5.el7_2.1
libreoffice-langpack-ro-4.3.7.2-5.el7_2.1
libreoffice-langpack-fa-4.3.7.2-5.el7_2.1
libreoffice-langpack-uk-4.3.7.2-5.el7_2.1
libreoffice-langpack-sk-4.3.7.2-5.el7_2.1
libreoffice-wiki-publisher-4.3.7.2-5.el7_2.1
libreoffice-filters-4.3.7.2-5.el7_2.1
libreoffice-langpack-he-4.3.7.2-5.el7_2.1
libreoffice-langpack-tr-4.3.7.2-5.el7_2.1
libreoffice-langpack-hu-4.3.7.2-5.el7_2.1
libreoffice-langpack-ca-4.3.7.2-5.el7_2.1
libreoffice-langpack-xh-4.3.7.2-5.el7_2.1
libreoffice-ogltrans-4.3.7.2-5.el7_2.1
libreoffice-langpack-zu-4.3.7.2-5.el7_2.1
libreoffice-langpack-si-4.3.7.2-5.el7_2.1
libreoffice-langpack-or-4.3.7.2-5.el7_2.1
libreoffice-langpack-bn-4.3.7.2-5.el7_2.1
libreoffice-langpack-kk-4.3.7.2-5.el7_2.1
libreoffice-base-4.3.7.2-5.el7_2.1

libreoffice-emailmerge-4.3.7.2-5.el7_2.1
libreoffice-langpack-mr-4.3.7.2-5.el7_2.1
libreoffice-bsh-4.3.7.2-5.el7_2.1
libreoffice-langpack-zh-Hant-4.3.7.2-5.el7_2.1
libreoffice-librelogo-4.3.7.2-5.el7_2.1
libreoffice-langpack-et-4.3.7.2-5.el7_2.1
libreoffice-langpack-af-4.3.7.2-5.el7_2.1
libreoffice-langpack-hr-4.3.7.2-5.el7_2.1
libreoffice-langpack-ga-4.3.7.2-5.el7_2.1
libreoffice-pyuno-4.3.7.2-5.el7_2.1
libreoffice-langpack-es-4.3.7.2-5.el7_2.1
libreoffice-langpack-cs-4.3.7.2-5.el7_2.1
libreoffice-langpack-fr-4.3.7.2-5.el7_2.1
libreoffice-impress-4.3.7.2-5.el7_2.1
libreoffice-langpack-pt-PT-4.3.7.2-5.el7_2.1
libreoffice-langpack-hi-4.3.7.2-5.el7_2.1
libreoffice-langpack-ja-4.3.7.2-5.el7_2.1
libreoffice-langpack-lt-4.3.7.2-5.el7_2.1
libreoffice-langpack-fi-4.3.7.2-5.el7_2.1
libreoffice-langpack-bg-4.3.7.2-5.el7_2.1
libreoffice-langpack-nso-4.3.7.2-5.el7_2.1
libreoffice-graphicfilter-4.3.7.2-5.el7_2.1
libreoffice-draw-4.3.7.2-5.el7_2.1
libreoffice-postgresql-4.3.7.2-5.el7_2.1
libreoffice-langpack-ko-4.3.7.2-5.el7_2.1
libreoffice-langpack-nn-4.3.7.2-5.el7_2.1
libreoffice-langpack-en-4.3.7.2-5.el7_2.1

noarch
autocorr-hu-4.3.7.2-5.el7_2.1
autocorr-tr-4.3.7.2-5.el7_2.1
autocorr-cs-4.3.7.2-5.el7_2.1
autocorr-sl-4.3.7.2-5.el7_2.1
autocorr-it-4.3.7.2-5.el7_2.1
autocorr-sv-4.3.7.2-5.el7_2.1
autocorr-sr-4.3.7.2-5.el7_2.1
autocorr-ru-4.3.7.2-5.el7_2.1
autocorr-fi-4.3.7.2-5.el7_2.1
autocorr-ja-4.3.7.2-5.el7_2.1
autocorr-pl-4.3.7.2-5.el7_2.1
autocorr-zh-4.3.7.2-5.el7_2.1
autocorr-af-4.3.7.2-5.el7_2.1
autocorr-fa-4.3.7.2-5.el7_2.1
autocorr-is-4.3.7.2-5.el7_2.1
autocorr-mn-4.3.7.2-5.el7_2.1
autocorr-ko-4.3.7.2-5.el7_2.1
autocorr-vi-4.3.7.2-5.el7_2.1
autocorr-fr-4.3.7.2-5.el7_2.1
libreoffice-opensymbol-fonts-4.3.7.2-5.el7_2.1
autocorr-ga-4.3.7.2-5.el7_2.1
autocorr-es-4.3.7.2-5.el7_2.1
autocorr-de-4.3.7.2-5.el7_2.1
autocorr-pt-4.3.7.2-5.el7_2.1
autocorr-hr-4.3.7.2-5.el7_2.1
autocorr-da-4.3.7.2-5.el7_2.1
autocorr-nl-4.3.7.2-5.el7_2.1
autocorr-lt-4.3.7.2-5.el7_2.1
autocorr-bg-4.3.7.2-5.el7_2.1
autocorr-lb-4.3.7.2-5.el7_2.1
autocorr-sk-4.3.7.2-5.el7_2.1

autocorr-ro-4.3.7.2-5.el7_2.1
autocorr-ca-4.3.7.2-5.el7_2.1
autocorr-en-4.3.7.2-5.el7_2.1

CentOS 6
i686
libreoffice-math-4.2.8.2-11.el6_7.1
libreoffice-langpack-tr-4.2.8.2-11.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.el6_7.1
libreoffice-langpack-ga-4.2.8.2-11.el6_7.1
libreoffice-langpack-sv-4.2.8.2-11.el6_7.1
libreoffice-langpack-fi-4.2.8.2-11.el6_7.1
libreoffice-headless-4.2.8.2-11.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.el6_7.1
libreoffice-langpack-pl-4.2.8.2-11.el6_7.1
libreoffice-filters-4.2.8.2-11.el6_7.1
libreoffice-langpack-kn-4.2.8.2-11.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.el6_7.1
libreoffice-langpack-lt-4.2.8.2-11.el6_7.1
libreoffice-draw-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hant-4.2.8.2-11.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.el6_7.1
libreoffice-langpack-or-4.2.8.2-11.el6_7.1
libreoffice-langpack-mai-4.2.8.2-11.el6_7.1
libreoffice-langpack-hu-4.2.8.2-11.el6_7.1
libreoffice-langpack-nr-4.2.8.2-11.el6_7.1
libreoffice-pyuno-4.2.8.2-11.el6_7.1
libreoffice-ure-4.2.8.2-11.el6_7.1
libreoffice-langpack-nl-4.2.8.2-11.el6_7.1
libreoffice-langpack-ca-4.2.8.2-11.el6_7.1
libreoffice-langpack-ro-4.2.8.2-11.el6_7.1
libreoffice-langpack-zu-4.2.8.2-11.el6_7.1
libreoffice-emailmerge-4.2.8.2-11.el6_7.1
libreoffice-glade-4.2.8.2-11.el6_7.1
libreoffice-langpack-bg-4.2.8.2-11.el6_7.1
libreoffice-librelogo-4.2.8.2-11.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.el6_7.1
libreoffice-langpack-ru-4.2.8.2-11.el6_7.1
libreoffice-langpack-da-4.2.8.2-11.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.el6_7.1
libreoffice-sdk-4.2.8.2-11.el6_7.1
libreoffice-langpack-as-4.2.8.2-11.el6_7.1
libreoffice-langpack-ta-4.2.8.2-11.el6_7.1
libreoffice-langpack-ur-4.2.8.2-11.el6_7.1
libreoffice-langpack-ve-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-PT-4.2.8.2-11.el6_7.1
libreoffice-base-4.2.8.2-11.el6_7.1
libreoffice-core-4.2.8.2-11.el6_7.1

170595 - Amazon Linux AMI ALAS-2015-621 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2014-4650, CVE-2014-7185

Description

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

ALAS-2015-621

Observation

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

https://alas.aws.amazon.com/ALAS-2015-621.html

Amazon Linux AMI
x86_64
python26-devel-2.6.9-2.83.amzn1
python26-2.6.9-2.83.amzn1
python26-libs-2.6.9-2.83.amzn1
python26-tools-2.6.9-2.83.amzn1
python26-debuginfo-2.6.9-2.83.amzn1
python26-test-2.6.9-2.83.amzn1

i686
python26-devel-2.6.9-2.83.amzn1
python26-2.6.9-2.83.amzn1
python26-debuginfo-2.6.9-2.83.amzn1
python26-tools-2.6.9-2.83.amzn1
python26-libs-2.6.9-2.83.amzn1
python26-test-2.6.9-2.83.amzn1

170598 - Amazon Linux AMI ALAS-2015-628 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317

Description

The scan detected that the host is missing the following update:
ALAS-2015-628

Observation

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

https://alas.aws.amazon.com/ALAS-2015-628.html

Amazon Linux AMI
x86_64
libxml2-python26-2.9.1-6.2.50.amzn1
libxml2-devel-2.9.1-6.2.50.amzn1
libxml2-static-2.9.1-6.2.50.amzn1
libxml2-2.9.1-6.2.50.amzn1
libxml2-python27-2.9.1-6.2.50.amzn1
libxml2-debuginfo-2.9.1-6.2.50.amzn1

i686
libxml2-python26-2.9.1-6.2.50.amzn1
libxml2-devel-2.9.1-6.2.50.amzn1
libxml2-static-2.9.1-6.2.50.amzn1
libxml2-2.9.1-6.2.50.amzn1
libxml2-python27-2.9.1-6.2.50.amzn1

libxml2-debuginfo-2.9.1-6.2.50.amzn1

170608 - Amazon Linux AMI ALAS-2015-619 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
ALAS-2015-619

Observation

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

https://alas.aws.amazon.com/ALAS-2015-619.html

Amazon Linux AMI
x86_64
postgresql8-test-8.4.20-4.51.amzn1
postgresql8-8.4.20-4.51.amzn1
postgresql8-server-8.4.20-4.51.amzn1
postgresql8-devel-8.4.20-4.51.amzn1
postgresql8-libs-8.4.20-4.51.amzn1
postgresql8-plperl-8.4.20-4.51.amzn1
postgresql8-docs-8.4.20-4.51.amzn1
postgresql8-debuginfo-8.4.20-4.51.amzn1
postgresql8-pltcl-8.4.20-4.51.amzn1
postgresql8-plpython-8.4.20-4.51.amzn1
postgresql8-contrib-8.4.20-4.51.amzn1

i686
postgresql8-pltcl-8.4.20-4.51.amzn1
postgresql8-8.4.20-4.51.amzn1
postgresql8-debuginfo-8.4.20-4.51.amzn1
postgresql8-devel-8.4.20-4.51.amzn1
postgresql8-libs-8.4.20-4.51.amzn1
postgresql8-plperl-8.4.20-4.51.amzn1
postgresql8-docs-8.4.20-4.51.amzn1
postgresql8-test-8.4.20-4.51.amzn1
postgresql8-server-8.4.20-4.51.amzn1
postgresql8-plpython-8.4.20-4.51.amzn1
postgresql8-contrib-8.4.20-4.51.amzn1

174719 - Scientific Linux Security ERRATA Important: openafs on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-13603)

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

Risk Level: Medium

CVE: CVE-2015-3282, CVE-2015-3283, CVE-2015-3284, CVE-2015-3285

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: openafs on SL5.x, SL6.x, SL7.x i386/x86_64 (1507-13603)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=13603

SL5
x86_64
openafs-kernel-source-1.4.15-86.sl5
openafs-krb5-1.4.15-86.sl5
openafs-client-1.4.15-86.sl5
kernel-module-openafs-2.6.18-406.el5xen-1.4.15-86.sl5
openafs-server-1.4.15-86.sl5
kernel-module-openafs-2.6.18-404.el5xen-1.4.15-86.sl5
openafs-authlibs-devel-1.4.15-86.sl5
openafs-compat-1.4.15-86.sl5
openafs-debug-1.4.15-86.sl5
openafs-devel-1.4.15-86.sl5
kernel-module-openafs-2.6.18-404.el5-1.4.15-86.sl5
openafs-1.4.15-86.sl5
openafs-authlibs-1.4.15-86.sl5
openafs-kpasswd-1.4.15-86.sl5
kernel-module-openafs-2.6.18-406.el5-1.4.15-86.sl5

i386
openafs-kernel-source-1.4.15-86.sl5
openafs-krb5-1.4.15-86.sl5
openafs-client-1.4.15-86.sl5
kernel-module-openafs-2.6.18-406.el5xen-1.4.15-86.sl5
openafs-server-1.4.15-86.sl5
kernel-module-openafs-2.6.18-404.el5xen-1.4.15-86.sl5
openafs-authlibs-devel-1.4.15-86.sl5
openafs-compat-1.4.15-86.sl5
openafs-debug-1.4.15-86.sl5
openafs-devel-1.4.15-86.sl5
kernel-module-openafs-2.6.18-406.el5PAE-1.4.15-86.sl5
kernel-module-openafs-2.6.18-404.el5-1.4.15-86.sl5
openafs-1.4.15-86.sl5
kernel-module-openafs-2.6.18-404.el5PAE-1.4.15-86.sl5
openafs-authlibs-1.4.15-86.sl5
openafs-kpasswd-1.4.15-86.sl5
kernel-module-openafs-2.6.18-406.el5-1.4.15-86.sl5

SL7
x86_64
openafs-1.6-sl-client-1.6.13-215.sl7
openafs-1.6-sl-krb5-1.6.13-215.sl7
openafs-1.6-sl-1.6.13-215.sl7
openafs-1.6-sl-kernel-source-1.6.13-215.sl7
openafs-1.6-sl-kpasswd-1.6.13-215.sl7
openafs-1.6-sl-devel-1.6.13-215.sl7
kmod-openafs-1.6-sl-229-1.6.13-215.sl7.229.1.2
openafs-1.6-sl-authlibs-1.6.13-215.sl7
openafs-1.6-sl-server-1.6.13-215.sl7
openafs-1.6-sl-plumbing-tools-1.6.13-215.sl7
openafs-1.6-sl-module-tools-1.6.13-215.sl7
openafs-1.6-sl-authlibs-devel-1.6.13-215.sl7
openafs-1.6-sl-compat-1.6.13-215.sl7

SL6
x86_64

openafs-kernel-source-1.6.13-215.sl6
openafs-authlibs-devel-1.6.13-215.sl6
openafs-module-tools-1.6.13-215.sl6
openafs-plumbing-tools-1.6.13-215.sl6
openafs-devel-1.6.13-215.sl6
openafs-authlibs-1.6.13-215.sl6
openafs-krb5-1.6.13-215.sl6
openafs-1.6.13-215.sl6
openafs-server-1.6.13-215.sl6
openafs-client-1.6.13-215.sl6
openafs-kpasswd-1.6.13-215.sl6
kmod-openafs-504-1.6.13-215.sl6.504
openafs-compat-1.6.13-215.sl6

i386
openafs-kernel-source-1.6.13-215.sl6
openafs-authlibs-devel-1.6.13-215.sl6
openafs-module-tools-1.6.13-215.sl6
openafs-plumbing-tools-1.6.13-215.sl6
openafs-devel-1.6.13-215.sl6
openafs-authlibs-1.6.13-215.sl6
openafs-krb5-1.6.13-215.sl6
openafs-1.6.13-215.sl6
openafs-server-1.6.13-215.sl6
openafs-client-1.6.13-215.sl6
openafs-kpasswd-1.6.13-215.sl6
kmod-openafs-504-1.6.13-215.sl6.504
openafs-compat-1.6.13-215.sl6

174720 - Scientific Linux Security ERRATA Important: libwmf on SL6.x, SL7.x i386/x86_64 (1510-2224)

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

Risk Level: Medium

CVE: CVE-2015-0848, CVE-2015-4588, CVE-2015-4695, CVE-2015-4696

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: libwmf on SL6.x, SL7.x i386/x86_64 (1510-2224)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=2224

SL7
x86_64
libwmf-lite-0.2.8.4-41.el7_1
libwmf-0.2.8.4-41.el7_1
libwmf-debuginfo-0.2.8.4-41.el7_1
libwmf-devel-0.2.8.4-41.el7_1

SL6
x86_64
libwmf-lite-0.2.8.4-25.el6_7
libwmf-devel-0.2.8.4-25.el6_7
libwmf-0.2.8.4-25.el6_7
libwmf-debuginfo-0.2.8.4-25.el6_7

i386
libwmf-lite-0.2.8.4-25.el6_7
libwmf-devel-0.2.8.4-25.el6_7
libwmf-0.2.8.4-25.el6_7
libwmf-debuginfo-0.2.8.4-25.el6_7

174737 - Scientific Linux Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1508-5487)

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

Risk Level: Medium

CVE: CVE-2015-1774

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1508-5487)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=5487

SL6
i386
libreoffice-langpack-st-4.2.8.2-11.el6
libreoffice-langpack-ss-4.2.8.2-11.el6
libreoffice-langpack-nb-4.2.8.2-11.el6
libreoffice-langpack-ro-4.2.8.2-11.el6
libreoffice-langpack-pl-4.2.8.2-11.el6
libreoffice-langpack-uk-4.2.8.2-11.el6
libreoffice-langpack-hr-4.2.8.2-11.el6
libreoffice-langpack-ms-4.2.8.2-11.el6
libreoffice-langpack-el-4.2.8.2-11.el6
libreoffice-pdfimport-4.2.8.2-11.el6
libreoffice-headless-4.2.8.2-11.el6
libreoffice-langpack-hu-4.2.8.2-11.el6
libreoffice-langpack-pa-4.2.8.2-11.el6
libreoffice-langpack-ar-4.2.8.2-11.el6
libreoffice-rhino-4.2.8.2-11.el6
libreoffice-core-4.2.8.2-11.el6
libreoffice-impress-4.2.8.2-11.el6
libreoffice-langpack-he-4.2.8.2-11.el6
libreoffice-wiki-publisher-4.2.8.2-11.el6
libreoffice-langpack-gl-4.2.8.2-11.el6
libreoffice-pyuno-4.2.8.2-11.el6
libreoffice-4.2.8.2-11.el6
libreoffice-emailmerge-4.2.8.2-11.el6
libreoffice-langpack-ve-4.2.8.2-11.el6
libreoffice-langpack-tn-4.2.8.2-11.el6
libreoffice-langpack-ga-4.2.8.2-11.el6
libreoffice-langpack-ts-4.2.8.2-11.el6
libreoffice-langpack-as-4.2.8.2-11.el6
libreoffice-langpack-fr-4.2.8.2-11.el6
libreoffice-glade-4.2.8.2-11.el6
libreoffice-langpack-kn-4.2.8.2-11.el6
libreoffice-sdk-4.2.8.2-11.el6
libreoffice-writer-4.2.8.2-11.el6
libreoffice-langpack-zh-Hans-4.2.8.2-11.el6

libreoffice-base-4.2.8.2-11.el6
libreoffice-langpack-dz-4.2.8.2-11.el6
libreoffice-langpack-tr-4.2.8.2-11.el6
libreoffice-nlpsolver-4.2.8.2-11.el6
libreoffice-sdk-doc-4.2.8.2-11.el6
libreoffice-langpack-th-4.2.8.2-11.el6
libreoffice-langpack-cs-4.2.8.2-11.el6
libreoffice-gdb-debug-support-4.2.8.2-11.el6
libreoffice-langpack-es-4.2.8.2-11.el6
libreoffice-langpack-et-4.2.8.2-11.el6
libreoffice-langpack-mai-4.2.8.2-11.el6
libreoffice-langpack-gu-4.2.8.2-11.el6
libreoffice-langpack-cy-4.2.8.2-11.el6
libreoffice-langpack-zu-4.2.8.2-11.el6
libreoffice-langpack-ta-4.2.8.2-11.el6
libreoffice-langpack-te-4.2.8.2-11.el6
libreoffice-langpack-xh-4.2.8.2-11.el6
libreoffice-librelogo-4.2.8.2-11.el6
libreoffice-langpack-nso-4.2.8.2-11.el6
libreoffice-langpack-fi-4.2.8.2-11.el6
libreoffice-langpack-bg-4.2.8.2-11.el6
libreoffice-langpack-eu-4.2.8.2-11.el6
libreoffice-langpack-sr-4.2.8.2-11.el6
libreoffice-filters-4.2.8.2-11.el6
libreoffice-langpack-sk-4.2.8.2-11.el6
libreoffice-langpack-sl-4.2.8.2-11.el6
libreoffice-langpack-da-4.2.8.2-11.el6
libreoffice-math-4.2.8.2-11.el6
libreoffice-debuginfo-4.2.8.2-11.el6
libreoffice-langpack-mr-4.2.8.2-11.el6
libreoffice-langpack-ja-4.2.8.2-11.el6
libreoffice-langpack-ko-4.2.8.2-11.el6
libreoffice-langpack-it-4.2.8.2-11.el6
libreoffice-langpack-ml-4.2.8.2-11.el6
libreoffice-graphicfilter-4.2.8.2-11.el6
libreoffice-xsltfilter-4.2.8.2-11.el6
libreoffice-ure-4.2.8.2-11.el6
libreoffice-langpack-hi-4.2.8.2-11.el6
libreoffice-langpack-pt-BR-4.2.8.2-11.el6
libreoffice-langpack-zh-Hant-4.2.8.2-11.el6
libreoffice-bsh-4.2.8.2-11.el6
libreoffice-langpack-lt-4.2.8.2-11.el6
libreoffice-langpack-or-4.2.8.2-11.el6
libreoffice-calc-4.2.8.2-11.el6
libreoffice-langpack-ru-4.2.8.2-11.el6
libreoffice-langpack-nn-4.2.8.2-11.el6
libreoffice-langpack-pt-PT-4.2.8.2-11.el6
libreoffice-langpack-sv-4.2.8.2-11.el6
libreoffice-langpack-ur-4.2.8.2-11.el6
libreoffice-ogltrans-4.2.8.2-11.el6
libreoffice-langpack-bn-4.2.8.2-11.el6
libreoffice-langpack-de-4.2.8.2-11.el6
libreoffice-langpack-ca-4.2.8.2-11.el6
libreoffice-langpack-en-4.2.8.2-11.el6
libreoffice-langpack-nr-4.2.8.2-11.el6
libreoffice-draw-4.2.8.2-11.el6
libreoffice-langpack-nl-4.2.8.2-11.el6
libreoffice-langpack-af-4.2.8.2-11.el6

noarch

autocorr-cs-4.2.8.2-11.el6
autocorr-sl-4.2.8.2-11.el6
autocorr-en-4.2.8.2-11.el6
autocorr-ca-4.2.8.2-11.el6
autocorr-lt-4.2.8.2-11.el6
autocorr-ga-4.2.8.2-11.el6
autocorr-es-4.2.8.2-11.el6
autocorr-it-4.2.8.2-11.el6
autocorr-bg-4.2.8.2-11.el6
autocorr-fi-4.2.8.2-11.el6
autocorr-da-4.2.8.2-11.el6
autocorr-de-4.2.8.2-11.el6
libreoffice-opensymbol-fonts-4.2.8.2-11.el6
autocorr-mn-4.2.8.2-11.el6
autocorr-ru-4.2.8.2-11.el6
autocorr-hr-4.2.8.2-11.el6
autocorr-pl-4.2.8.2-11.el6
autocorr-hu-4.2.8.2-11.el6
autocorr-nl-4.2.8.2-11.el6
autocorr-is-4.2.8.2-11.el6
autocorr-fr-4.2.8.2-11.el6
autocorr-ro-4.2.8.2-11.el6
autocorr-ko-4.2.8.2-11.el6
autocorr-fa-4.2.8.2-11.el6
autocorr-pt-4.2.8.2-11.el6
autocorr-tr-4.2.8.2-11.el6
autocorr-af-4.2.8.2-11.el6
autocorr-vi-4.2.8.2-11.el6
autocorr-sk-4.2.8.2-11.el6
autocorr-lb-4.2.8.2-11.el6
autocorr-ja-4.2.8.2-11.el6
autocorr-zh-4.2.8.2-11.el6
autocorr-sr-4.2.8.2-11.el6
autocorr-sv-4.2.8.2-11.el6

x86_64
libreoffice-langpack-st-4.2.8.2-11.el6
libreoffice-langpack-ss-4.2.8.2-11.el6
libreoffice-langpack-nb-4.2.8.2-11.el6
libreoffice-langpack-ro-4.2.8.2-11.el6
libreoffice-langpack-pl-4.2.8.2-11.el6
libreoffice-langpack-uk-4.2.8.2-11.el6
libreoffice-langpack-hr-4.2.8.2-11.el6
libreoffice-langpack-ms-4.2.8.2-11.el6
libreoffice-langpack-el-4.2.8.2-11.el6
libreoffice-pdfimport-4.2.8.2-11.el6
libreoffice-headless-4.2.8.2-11.el6
libreoffice-langpack-hu-4.2.8.2-11.el6
libreoffice-langpack-pa-4.2.8.2-11.el6
libreoffice-langpack-ar-4.2.8.2-11.el6
libreoffice-rhino-4.2.8.2-11.el6
libreoffice-core-4.2.8.2-11.el6
libreoffice-impress-4.2.8.2-11.el6
libreoffice-langpack-he-4.2.8.2-11.el6
libreoffice-wiki-publisher-4.2.8.2-11.el6
libreoffice-langpack-gl-4.2.8.2-11.el6
libreoffice-pyuno-4.2.8.2-11.el6
libreoffice-4.2.8.2-11.el6
libreoffice-emailmerge-4.2.8.2-11.el6
libreoffice-langpack-ve-4.2.8.2-11.el6

libreoffice-langpack-tn-4.2.8.2-11.el6
libreoffice-langpack-ga-4.2.8.2-11.el6
libreoffice-langpack-ts-4.2.8.2-11.el6
libreoffice-langpack-as-4.2.8.2-11.el6
libreoffice-langpack-fr-4.2.8.2-11.el6
libreoffice-glade-4.2.8.2-11.el6
libreoffice-langpack-kn-4.2.8.2-11.el6
libreoffice-sdk-4.2.8.2-11.el6
libreoffice-writer-4.2.8.2-11.el6
libreoffice-langpack-zh-Hans-4.2.8.2-11.el6
libreoffice-base-4.2.8.2-11.el6
libreoffice-langpack-dz-4.2.8.2-11.el6
libreoffice-langpack-tr-4.2.8.2-11.el6
libreoffice-nlpsolver-4.2.8.2-11.el6
libreoffice-sdk-doc-4.2.8.2-11.el6
libreoffice-langpack-th-4.2.8.2-11.el6
libreoffice-langpack-cs-4.2.8.2-11.el6
libreoffice-gdb-debug-support-4.2.8.2-11.el6
libreoffice-langpack-es-4.2.8.2-11.el6
libreoffice-langpack-et-4.2.8.2-11.el6
libreoffice-langpack-mai-4.2.8.2-11.el6
libreoffice-langpack-gu-4.2.8.2-11.el6
libreoffice-langpack-cy-4.2.8.2-11.el6
libreoffice-langpack-zu-4.2.8.2-11.el6
libreoffice-langpack-ta-4.2.8.2-11.el6
libreoffice-langpack-te-4.2.8.2-11.el6
libreoffice-langpack-xh-4.2.8.2-11.el6
libreoffice-librelogo-4.2.8.2-11.el6
libreoffice-langpack-nso-4.2.8.2-11.el6
libreoffice-langpack-fi-4.2.8.2-11.el6
libreoffice-langpack-bg-4.2.8.2-11.el6
libreoffice-langpack-eu-4.2.8.2-11.el6
libreoffice-langpack-sr-4.2.8.2-11.el6
libreoffice-filters-4.2.8.2-11.el6
libreoffice-langpack-sk-4.2.8.2-11.el6
libreoffice-langpack-sl-4.2.8.2-11.el6
libreoffice-langpack-da-4.2.8.2-11.el6
libreoffice-math-4.2.8.2-11.el6
libreoffice-debuginfo-4.2.8.2-11.el6

174745 - Scientific Linux Security ERRATA Moderate: gdk-pixbuf2 on SL6.x, SL7.x i386/x86_64 (1508-24877)

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

Risk Level: Medium

CVE: CVE-2015-4491

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gdk-pixbuf2 on SL6.x, SL7.x i386/x86_64 (1508-24877)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=24877

SL7
x86_64

gdk-pixbuf2-2.28.2-5.el7_1
gdk-pixbuf2-debuginfo-2.28.2-5.el7_1
gdk-pixbuf2-devel-2.28.2-5.el7_1

SL6
x86_64
gdk-pixbuf2-devel-2.24.1-6.el6_7
gdk-pixbuf2-debuginfo-2.24.1-6.el6_7
gdk-pixbuf2-2.24.1-6.el6_7

i386
gdk-pixbuf2-devel-2.24.1-6.el6_7
gdk-pixbuf2-debuginfo-2.24.1-6.el6_7
gdk-pixbuf2-2.24.1-6.el6_7

174749 - Scientific Linux Security ERRATA Moderate: libxml2 on SL6.x i386/x86_64 (1512-79)

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

Risk Level: Medium

CVE: CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libxml2 on SL6.x i386/x86_64 (1512-79)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=79

SL6
x86_64
libxml2-2.7.6-20.el6_7.1
libxml2-debuginfo-2.7.6-20.el6_7.1
libxml2-static-2.7.6-20.el6_7.1
libxml2-python-2.7.6-20.el6_7.1
libxml2-devel-2.7.6-20.el6_7.1

i386
libxml2-2.7.6-20.el6_7.1
libxml2-debuginfo-2.7.6-20.el6_7.1
libxml2-static-2.7.6-20.el6_7.1
libxml2-python-2.7.6-20.el6_7.1
libxml2-devel-2.7.6-20.el6_7.1

174753 - Scientific Linux Security ERRATA Moderate: kernel on SL7.x x86_64 (1511-449)

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

Risk Level: Medium

CVE: CVE-2014-8559, CVE-2015-5156

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL7.x x86_64 (1511-449)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=449

SL7
x86_64
perf-3.10.0-229.20.1.el7
python-perf-3.10.0-229.20.1.el7
kernel-debug-3.10.0-229.20.1.el7
python-perf-debuginfo-3.10.0-229.20.1.el7
kernel-devel-3.10.0-229.20.1.el7
kernel-debuginfo-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.20.1.el7
kernel-debug-debuginfo-3.10.0-229.20.1.el7
kernel-tools-debuginfo-3.10.0-229.20.1.el7
kernel-tools-libs-devel-3.10.0-229.20.1.el7
perf-debuginfo-3.10.0-229.20.1.el7
kernel-debug-devel-3.10.0-229.20.1.el7
kernel-tools-3.10.0-229.20.1.el7
kernel-3.10.0-229.20.1.el7
kernel-tools-libs-3.10.0-229.20.1.el7

noarch
kernel-doc-3.10.0-229.20.1.el7
kernel-abi-whitelists-3.10.0-229.20.1.el7

174757 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1512-1991)

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-5307, CVE-2015-7613, CVE-2015-7872, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1512-1991)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=1991

SL6
i386
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
perf-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6

perf-debuginfo-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6

noarch
kernel-abi-whitelists-2.6.32-573.12.1.el6
kernel-doc-2.6.32-573.12.1.el6
kernel-firmware-2.6.32-573.12.1.el6

x86_64
perf-2.6.32-573.12.1.el6
perf-debuginfo-2.6.32-573.12.1.el6
kernel-headers-2.6.32-573.12.1.el6
python-perf-2.6.32-573.12.1.el6
python-perf-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-2.6.32-573.12.1.el6
kernel-debuginfo-common-i686-2.6.32-573.12.1.el6
kernel-devel-2.6.32-573.12.1.el6
kernel-2.6.32-573.12.1.el6
kernel-debug-devel-2.6.32-573.12.1.el6
kernel-debuginfo-common-x86_64-2.6.32-573.12.1.el6
kernel-debug-2.6.32-573.12.1.el6
kernel-debug-debuginfo-2.6.32-573.12.1.el6

174761 - Scientific Linux Security ERRATA Important: spice-server on SL6.x x86_64 (1509-7881)

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

Risk Level: Medium

CVE: CVE-2015-3247

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice-server on SL6.x x86_64 (1509-7881)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=7881

SL6
x86_64
spice-server-debuginfo-0.12.4-12.el6_7.1
spice-server-devel-0.12.4-12.el6_7.1
spice-server-0.12.4-12.el6_7.1

174780 - Scientific Linux Security ERRATA Important: spice-server on SL7.x x86_64 (1509-7545)

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

Risk Level: Medium

CVE: CVE-2015-3247

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: spice-server on SL7.x x86_64 (1509-7545)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=7545

SL7
x86_64
spice-server-devel-0.12.4-9.el7_1.1
spice-debuginfo-0.12.4-9.el7_1.1
spice-server-0.12.4-9.el7_1.1

174785 - Scientific Linux Security ERRATA Moderate: postgresql on SL6.x i386/x86_64 (1511-14456)

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL6.x i386/x86_64 (1511-14456)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=14456

SL6
x86_64
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

i386
postgresql-devel-8.4.20-4.el6_7
postgresql-libs-8.4.20-4.el6_7
postgresql-8.4.20-4.el6_7
postgresql-server-8.4.20-4.el6_7
postgresql-docs-8.4.20-4.el6_7
postgresql-contrib-8.4.20-4.el6_7
postgresql-plperl-8.4.20-4.el6_7
postgresql-test-8.4.20-4.el6_7
postgresql-debuginfo-8.4.20-4.el6_7
postgresql-pltcl-8.4.20-4.el6_7
postgresql-plpython-8.4.20-4.el6_7

174789 - Scientific Linux Security ERRATA Moderate: postgresql on SL7.x srpm/x86_64 (1511-15417)

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL7.x srpm/x86_64 (1511-15417)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=15417

SL7
x86_64
postgresql-test-9.2.14-1.el7_1
postgresql-9.2.14-1.el7_1
postgresql-plperl-9.2.14-1.el7_1
postgresql-plpython-9.2.14-1.el7_1
postgresql-pltcl-9.2.14-1.el7_1
postgresql-upgrade-9.2.14-1.el7_1
postgresql-libs-9.2.14-1.el7_1
postgresql-server-9.2.14-1.el7_1
postgresql-docs-9.2.14-1.el7_1
postgresql-contrib-9.2.14-1.el7_1
postgresql-devel-9.2.14-1.el7_1
postgresql-debuginfo-9.2.14-1.el7_1

174794 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1508-7966)

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

Risk Level: Medium

CVE: CVE-2014-3184, CVE-2014-3940, CVE-2014-4652, CVE-2014-8133, CVE-2014-8709, CVE-2014-9683, CVE-2015-0239, CVE-2015-3339

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1508-7966)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=7966

SL6
i386
perf-debuginfo-2.6.32-573.el6
perf-2.6.32-573.el6
python-perf-2.6.32-573.el6
python-perf-debuginfo-2.6.32-573.el6
kernel-headers-2.6.32-573.el6
kernel-2.6.32-573.el6
kernel-devel-2.6.32-573.el6
kernel-debuginfo-2.6.32-573.el6
kernel-debug-2.6.32-573.el6
kernel-debug-devel-2.6.32-573.el6

kernel-debug-debuginfo-2.6.32-573.el6
kernel-debuginfo-common-i686-2.6.32-573.el6

noarch
kernel-doc-2.6.32-573.el6
kernel-abi-whitelists-2.6.32-573.el6
kernel-firmware-2.6.32-573.el6

x86_64
perf-debuginfo-2.6.32-573.el6
perf-2.6.32-573.el6
kernel-debuginfo-common-x86_64-2.6.32-573.el6
python-perf-debuginfo-2.6.32-573.el6
kernel-headers-2.6.32-573.el6
kernel-2.6.32-573.el6
kernel-devel-2.6.32-573.el6
kernel-debuginfo-2.6.32-573.el6
kernel-debug-2.6.32-573.el6
kernel-debug-devel-2.6.32-573.el6
kernel-debug-debuginfo-2.6.32-573.el6
python-perf-2.6.32-573.el6

174805 - Scientific Linux Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1512-1605)

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

Risk Level: Medium

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreoffice on SL6.x i386/x86_64 (1512-1605)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=1605

SL6
i386
libreoffice-math-4.2.8.2-11.el6_7.1
libreoffice-langpack-tr-4.2.8.2-11.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.el6_7.1
libreoffice-langpack-ga-4.2.8.2-11.el6_7.1
libreoffice-langpack-sv-4.2.8.2-11.el6_7.1
libreoffice-langpack-fi-4.2.8.2-11.el6_7.1
libreoffice-headless-4.2.8.2-11.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.el6_7.1
libreoffice-langpack-pl-4.2.8.2-11.el6_7.1
libreoffice-langpack-mr-4.2.8.2-11.el6_7.1
libreoffice-langpack-kn-4.2.8.2-11.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.el6_7.1
libreoffice-langpack-lt-4.2.8.2-11.el6_7.1
libreoffice-draw-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hant-4.2.8.2-11.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.el6_7.1
libreoffice-langpack-or-4.2.8.2-11.el6_7.1

libreoffice-langpack-mai-4.2.8.2-11.el6_7.1
libreoffice-langpack-nr-4.2.8.2-11.el6_7.1
libreoffice-pyuno-4.2.8.2-11.el6_7.1
libreoffice-ure-4.2.8.2-11.el6_7.1
libreoffice-langpack-nl-4.2.8.2-11.el6_7.1
libreoffice-langpack-ca-4.2.8.2-11.el6_7.1
libreoffice-langpack-zu-4.2.8.2-11.el6_7.1
libreoffice-debuginfo-4.2.8.2-11.el6_7.1
libreoffice-emailmerge-4.2.8.2-11.el6_7.1
libreoffice-langpack-ro-4.2.8.2-11.el6_7.1
libreoffice-langpack-bg-4.2.8.2-11.el6_7.1
libreoffice-librelogo-4.2.8.2-11.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.el6_7.1
libreoffice-langpack-ru-4.2.8.2-11.el6_7.1
libreoffice-langpack-da-4.2.8.2-11.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.el6_7.1
libreoffice-sdk-4.2.8.2-11.el6_7.1
libreoffice-langpack-hu-4.2.8.2-11.el6_7.1
libreoffice-langpack-ta-4.2.8.2-11.el6_7.1
libreoffice-langpack-ur-4.2.8.2-11.el6_7.1
libreoffice-langpack-ve-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-PT-4.2.8.2-11.el6_7.1
libreoffice-base-4.2.8.2-11.el6_7.1
libreoffice-core-4.2.8.2-11.el6_7.1
libreoffice-langpack-as-4.2.8.2-11.el6_7.1
libreoffice-langpack-pa-4.2.8.2-11.el6_7.1
libreoffice-sdk-doc-4.2.8.2-11.el6_7.1
libreoffice-langpack-cs-4.2.8.2-11.el6_7.1
libreoffice-rhino-4.2.8.2-11.el6_7.1
libreoffice-gdb-debug-support-4.2.8.2-11.el6_7.1
libreoffice-langpack-ss-4.2.8.2-11.el6_7.1
libreoffice-langpack-bn-4.2.8.2-11.el6_7.1
libreoffice-langpack-hi-4.2.8.2-11.el6_7.1
libreoffice-langpack-ar-4.2.8.2-11.el6_7.1
libreoffice-langpack-xh-4.2.8.2-11.el6_7.1
libreoffice-impress-4.2.8.2-11.el6_7.1
libreoffice-ogltrans-4.2.8.2-11.el6_7.1
libreoffice-filters-4.2.8.2-11.el6_7.1
libreoffice-xsltfilter-4.2.8.2-11.el6_7.1
libreoffice-graphicfilter-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hans-4.2.8.2-11.el6_7.1
libreoffice-wiki-publisher-4.2.8.2-11.el6_7.1
libreoffice-langpack-ts-4.2.8.2-11.el6_7.1
libreoffice-langpack-tn-4.2.8.2-11.el6_7.1
libreoffice-calc-4.2.8.2-11.el6_7.1
libreoffice-langpack-nb-4.2.8.2-11.el6_7.1
libreoffice-langpack-nso-4.2.8.2-11.el6_7.1
libreoffice-langpack-sl-4.2.8.2-11.el6_7.1
libreoffice-glade-4.2.8.2-11.el6_7.1
libreoffice-nlpsolver-4.2.8.2-11.el6_7.1
libreoffice-langpack-de-4.2.8.2-11.el6_7.1
libreoffice-langpack-dz-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-BR-4.2.8.2-11.el6_7.1
libreoffice-writer-4.2.8.2-11.el6_7.1
libreoffice-langpack-te-4.2.8.2-11.el6_7.1
libreoffice-langpack-et-4.2.8.2-11.el6_7.1
libreoffice-langpack-eu-4.2.8.2-11.el6_7.1
libreoffice-bsh-4.2.8.2-11.el6_7.1
libreoffice-langpack-cy-4.2.8.2-11.el6_7.1

libreoffice-langpack-hr-4.2.8.2-11.el6_7.1
libreoffice-langpack-nn-4.2.8.2-11.el6_7.1
libreoffice-4.2.8.2-11.el6_7.1
libreoffice-langpack-he-4.2.8.2-11.el6_7.1
libreoffice-langpack-sr-4.2.8.2-11.el6_7.1
libreoffice-langpack-en-4.2.8.2-11.el6_7.1
libreoffice-langpack-ml-4.2.8.2-11.el6_7.1
libreoffice-langpack-it-4.2.8.2-11.el6_7.1
libreoffice-langpack-gu-4.2.8.2-11.el6_7.1
libreoffice-langpack-th-4.2.8.2-11.el6_7.1
libreoffice-langpack-ms-4.2.8.2-11.el6_7.1
libreoffice-pdfimport-4.2.8.2-11.el6_7.1
libreoffice-langpack-ko-4.2.8.2-11.el6_7.1
libreoffice-langpack-st-4.2.8.2-11.el6_7.1

noarch
autocorr-cs-4.2.8.2-11.el6_7.1
autocorr-en-4.2.8.2-11.el6_7.1
autocorr-is-4.2.8.2-11.el6_7.1
autocorr-ja-4.2.8.2-11.el6_7.1
autocorr-sk-4.2.8.2-11.el6_7.1
autocorr-vi-4.2.8.2-11.el6_7.1
autocorr-af-4.2.8.2-11.el6_7.1
autocorr-da-4.2.8.2-11.el6_7.1
autocorr-es-4.2.8.2-11.el6_7.1
autocorr-fa-4.2.8.2-11.el6_7.1
libreoffice-opensymbol-fonts-4.2.8.2-11.el6_7.1
autocorr-lt-4.2.8.2-11.el6_7.1
autocorr-it-4.2.8.2-11.el6_7.1
autocorr-sl-4.2.8.2-11.el6_7.1
autocorr-ro-4.2.8.2-11.el6_7.1
autocorr-hu-4.2.8.2-11.el6_7.1
autocorr-tr-4.2.8.2-11.el6_7.1
autocorr-fi-4.2.8.2-11.el6_7.1
autocorr-ko-4.2.8.2-11.el6_7.1
autocorr-mn-4.2.8.2-11.el6_7.1
autocorr-bg-4.2.8.2-11.el6_7.1
autocorr-ga-4.2.8.2-11.el6_7.1
autocorr-pt-4.2.8.2-11.el6_7.1
autocorr-sr-4.2.8.2-11.el6_7.1
autocorr-ca-4.2.8.2-11.el6_7.1
autocorr-ru-4.2.8.2-11.el6_7.1
autocorr-hr-4.2.8.2-11.el6_7.1
autocorr-lb-4.2.8.2-11.el6_7.1
autocorr-nl-4.2.8.2-11.el6_7.1
autocorr-de-4.2.8.2-11.el6_7.1
autocorr-zh-4.2.8.2-11.el6_7.1
autocorr-sv-4.2.8.2-11.el6_7.1
autocorr-pl-4.2.8.2-11.el6_7.1
autocorr-fr-4.2.8.2-11.el6_7.1

x86_64
libreoffice-math-4.2.8.2-11.el6_7.1
libreoffice-langpack-tr-4.2.8.2-11.el6_7.1
libreoffice-langpack-sk-4.2.8.2-11.el6_7.1
libreoffice-langpack-ga-4.2.8.2-11.el6_7.1
libreoffice-langpack-sv-4.2.8.2-11.el6_7.1
libreoffice-langpack-fi-4.2.8.2-11.el6_7.1
libreoffice-headless-4.2.8.2-11.el6_7.1
libreoffice-langpack-el-4.2.8.2-11.el6_7.1

libreoffice-langpack-pl-4.2.8.2-11.el6_7.1
libreoffice-langpack-mr-4.2.8.2-11.el6_7.1
libreoffice-langpack-kn-4.2.8.2-11.el6_7.1
libreoffice-langpack-es-4.2.8.2-11.el6_7.1
libreoffice-langpack-ja-4.2.8.2-11.el6_7.1
libreoffice-langpack-lt-4.2.8.2-11.el6_7.1
libreoffice-draw-4.2.8.2-11.el6_7.1
libreoffice-langpack-zh-Hant-4.2.8.2-11.el6_7.1
libreoffice-langpack-gl-4.2.8.2-11.el6_7.1
libreoffice-langpack-or-4.2.8.2-11.el6_7.1
libreoffice-langpack-mai-4.2.8.2-11.el6_7.1
libreoffice-langpack-nr-4.2.8.2-11.el6_7.1
libreoffice-pyuno-4.2.8.2-11.el6_7.1
libreoffice-ure-4.2.8.2-11.el6_7.1
libreoffice-langpack-nl-4.2.8.2-11.el6_7.1
libreoffice-langpack-ca-4.2.8.2-11.el6_7.1
libreoffice-langpack-zu-4.2.8.2-11.el6_7.1
libreoffice-debuginfo-4.2.8.2-11.el6_7.1
libreoffice-emailmerge-4.2.8.2-11.el6_7.1
libreoffice-langpack-ro-4.2.8.2-11.el6_7.1
libreoffice-langpack-bg-4.2.8.2-11.el6_7.1
libreoffice-librelogo-4.2.8.2-11.el6_7.1
libreoffice-langpack-af-4.2.8.2-11.el6_7.1
libreoffice-langpack-fr-4.2.8.2-11.el6_7.1
libreoffice-langpack-ru-4.2.8.2-11.el6_7.1
libreoffice-langpack-da-4.2.8.2-11.el6_7.1
libreoffice-langpack-uk-4.2.8.2-11.el6_7.1
libreoffice-sdk-4.2.8.2-11.el6_7.1
libreoffice-langpack-hu-4.2.8.2-11.el6_7.1
libreoffice-langpack-ta-4.2.8.2-11.el6_7.1
libreoffice-langpack-ur-4.2.8.2-11.el6_7.1
libreoffice-langpack-ve-4.2.8.2-11.el6_7.1
libreoffice-langpack-pt-PT-4.2.8.2-11.el6_7.1
libreoffice-base-4.2.8.2-11.el6_7.1
libreoffice-core-4.2.8.2-11.el6_7.1
libreoffice-langpack-as-4.2.8.2-11.el6_7.1
libreoffice-langpack-pa-4.2.8.2-11.el6_7.1

174809 - Scientific Linux Security ERRATA Moderate: kernel on SL7.x x86_64 (1508-9022)

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

Risk Level: Medium

CVE: CVE-2014-9715, CVE-2015-2666, CVE-2015-2922, CVE-2015-3636

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL7.x x86_64 (1508-9022)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=9022

SL7
x86_64
kernel-tools-debuginfo-3.10.0-229.11.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.11.1.el7

kernel-tools-libs-devel-3.10.0-229.11.1.el7
kernel-debuginfo-3.10.0-229.11.1.el7
perf-debuginfo-3.10.0-229.11.1.el7
kernel-3.10.0-229.11.1.el7
perf-3.10.0-229.11.1.el7
kernel-debug-3.10.0-229.11.1.el7
python-perf-3.10.0-229.11.1.el7
kernel-tools-3.10.0-229.11.1.el7
kernel-headers-3.10.0-229.11.1.el7
kernel-devel-3.10.0-229.11.1.el7
kernel-debug-devel-3.10.0-229.11.1.el7
kernel-debug-debuginfo-3.10.0-229.11.1.el7
kernel-tools-libs-3.10.0-229.11.1.el7
python-perf-debuginfo-3.10.0-229.11.1.el7

noarch
kernel-doc-3.10.0-229.11.1.el7
kernel-abi-whitelists-3.10.0-229.11.1.el7

174831 - Scientific Linux Security ERRATA Low: sssd on SL6.x i386/x86_64 (1511-2022)

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: sssd on SL6.x i386/x86_64 (1511-2022)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=2022

SL6
i386
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4

sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

noarch
python-sssdconfig-1.12.4-47.el6_7.4

x86_64
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

178071 - Gentoo Linux GLSA-201505-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4986, CVE-2014-4987, CVE-2014-6300, CVE-2014-8958, CVE-2014-8959, CVE-2014-8960, CVE-2014-8961

Description

The scan detected that the host is missing the following update:
GLSA-201505-03

Observation

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

https://security.gentoo.org/glsa/201505-03

Affected packages:
dev-db/phpmyadmin < 4.2.13

178075 - Gentoo Linux GLSA-201507-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1793

Description

The scan detected that the host is missing the following update:
GLSA-201507-15

Observation

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

https://security.gentoo.org/glsa/201507-15

Affected packages:
dev-libs/openssl < 1.0.1p

178093 - Gentoo Linux GLSA-201504-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103, CVE-2015-0255

Description

The scan detected that the host is missing the following update:
GLSA-201504-06

Observation

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

https://security.gentoo.org/glsa/201504-06

Affected packages:
x11-base/xorg-server < 1.12.4-r4

178102 - Gentoo Linux GLSA-201504-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5704, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231

Description

The scan detected that the host is missing the following update:
GLSA-201504-03

Observation

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

https://security.gentoo.org/glsa/201504-03

Affected packages:
www-servers/apache < 2.2.29

178124 - Gentoo Linux GLSA-201507-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1821, CVE-2015-1822, CVE-2015-1853

Description

The scan detected that the host is missing the following update:
GLSA-201507-01

Observation

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

https://security.gentoo.org/glsa/201507-01

Affected packages:
net-misc/chrony < 1.31.1

19327 - Splunk Enterprise Denial of Service Vulnerability Prior To 6.2.7

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

Risk Level: Medium

CVE: CVE-2015-1609

Description

A denial of service vulnerability is present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for the real-time operational intelligence.

A denial of service vulnerability is present in some versions of Splunk Enterprise. The flaw lies in KV store. Successful exploitation could allow an attacker to cause denial of service.

19429 - Schneider Electric ProClima ActiveX Control Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2015-7918

Description

A vulnerability in some versions of Schneider Electric ProClima could lead to remote code execution.

Observation

A vulnerability in some versions of Schneider Electric ProClima could lead to remote code execution.

The flaw lies in ActiveX Controls associated with Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

19430 - (HPSBGN03521) HP Operations Orchestration Central Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-5451

Description

A cross-site request forgery (CSRF) vulnerability is present in some versions of HP Operations Orchestration.

Observation

HP Operations Orchestration is a product for IT automated tasks coordination.

A cross-site request forgery (CSRF) vulnerability is present in some versions of HP Operations Orchestration. The flaw is due to an incorrect validation process of web requests. Successful exploitation could allow an attacker to retrieve sensitive information or to cause a denial of service condition.

88724 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-349-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1794, CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
SSA:2015-349-04

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.754583

Slackware 14.0
x86_64
openssl-1.0.1q-x86_64-1
openssl-solibs-1.0.1q-x86_64-1

Slackware 13.0
x86_64
openssl-0.9.8zh-x86_64-1
openssl-solibs-0.9.8zh-x86_64-1

Slackware 13.1
x86_64
openssl-0.9.8zh-x86_64-1
openssl-solibs-0.9.8zh-x86_64-1

Slackware 14.1
x86_64
openssl-1.0.1q-x86_64-1
openssl-solibs-1.0.1q-x86_64-1

Slackware 13.37
x86_64
openssl-0.9.8zh-x86_64-1
openssl-solibs-0.9.8zh-x86_64-1

88727 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-349-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3193, CVE-2015-8000, CVE-2015-8461

Description

The scan detected that the host is missing the following update:
SSA:2015-349-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.539966

Slackware 14.0
x86_64
bind-9.9.8_P2-x86_64-1

Slackware 13.0
x86_64
bind-9.9.8_P2-x86_64-1

Slackware 13.1
x86_64
bind-9.9.8_P2-x86_64-1

Slackware 14.1
x86_64
bind-9.9.8_P2-x86_64-1

Slackware 13.37
x86_64
bind-9.9.8_P2-x86_64-1

91976 - Oracle Enterprise Linux ELSA-2015-2616 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2015-3195

Description

The scan detected that the host is missing the following update:
ELSA-2015-2616

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005627.html

OEL5
x86_64
openssl-perl-0.9.8e-37.0.1.el5_11
openssl-devel-0.9.8e-37.0.1.el5_11
openssl-0.9.8e-37.0.1.el5_11

i386
openssl-perl-0.9.8e-37.0.1.el5_11
openssl-devel-0.9.8e-37.0.1.el5_11
openssl-0.9.8e-37.0.1.el5_11

91983 - Oracle Enterprise Linux ELSA-2015-2623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
ELSA-2015-2623

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005630.html

OEL7
x86_64
grub2-efi-modules-2.02-0.33.0.1.el7_2
grub2-2.02-0.33.0.1.el7_2
grub2-tools-2.02-0.33.0.1.el7_2
grub2-efi-2.02-0.33.0.1.el7_2

130336 - Debian Linux 7.0, 8.0 DSA-3417-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7940

Description

The scan detected that the host is missing the following update:
DSA-3417-1

Observation

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

http://www.debian.org/security/2015/dsa-3417

Debian 8.0
all
libbcpg-java-doc_1.49+dfsg-3+deb8u1
libbcmail-java_1.49+dfsg-3+deb8u1
libbcpg-java_1.49+dfsg-3+deb8u1
libbcmail-java-doc_1.49+dfsg-3+deb8u1
libbcpkix-java-doc_1.49+dfsg-3+deb8u1
libbcpkix-java_1.49+dfsg-3+deb8u1
libbcprov-java-doc_1.49+dfsg-3+deb8u1
libbcprov-java_1.49+dfsg-3+deb8u1

Debian 7.0
all
libbctsp-java-gcj_1.44+dfsg-3.1+deb7u1
libbcpg-java_1.44+dfsg-3.1+deb7u1
libbcmail-java_1.44+dfsg-3.1+deb7u1
libbcpg-java-gcj_1.44+dfsg-3.1+deb7u1

libbcprov-java_1.44+dfsg-3.1+deb7u1
libbcprov-java-doc_1.44+dfsg-3.1+deb7u1
libbctsp-java-doc_1.44+dfsg-3.1+deb7u1
libbcprov-java-gcj_1.44+dfsg-3.1+deb7u1
libbctsp-java_1.44+dfsg-3.1+deb7u1
libbcpg-java-doc_1.44+dfsg-3.1+deb7u1
libbcmail-java-doc_1.44+dfsg-3.1+deb7u1
libbcmail-java-gcj_1.44+dfsg-3.1+deb7u1

132204 - Oracle VM OVMSA-2015-0155 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0155

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-December/000403.html

OVM3.3
x86_64
openssl-1.0.1e-42.el6_7.1

141033 - Red Hat Enterprise Linux RHSA-2015-2616 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3195

Description

The scan detected that the host is missing the following update:
RHSA-2015-2616

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2616.html

RHEL5D
x86_64
openssl-debuginfo-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

i386
openssl-debuginfo-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

RHEL5S
i386
openssl-debuginfo-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

x86_64
openssl-debuginfo-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

141037 - Red Hat Enterprise Linux RHSA-2015-2617 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
RHSA-2015-2617

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2617.html

RHEL6S
i386
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

x86_64
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

RHEL6WS
x86_64
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

i386
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

RHEL7D
x86_64
openssl-libs-1.0.1e-51.el7_2.1

openssl-devel-1.0.1e-51.el7_2.1
openssl-debuginfo-1.0.1e-51.el7_2.1
openssl-1.0.1e-51.el7_2.1
openssl-static-1.0.1e-51.el7_2.1
openssl-perl-1.0.1e-51.el7_2.1

RHEL6D
x86_64
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

i386
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

RHEL7WS
x86_64
openssl-libs-1.0.1e-51.el7_2.1
openssl-devel-1.0.1e-51.el7_2.1
openssl-debuginfo-1.0.1e-51.el7_2.1
openssl-1.0.1e-51.el7_2.1
openssl-static-1.0.1e-51.el7_2.1
openssl-perl-1.0.1e-51.el7_2.1

141039 - Red Hat Enterprise Linux RHSA-2015-2623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
RHSA-2015-2623

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2623.html

RHEL7D
x86_64
grub2-debuginfo-2.02-0.33.el7_2
grub2-tools-2.02-0.33.el7_2
grub2-2.02-0.33.el7_2
grub2-efi-2.02-0.33.el7_2
grub2-efi-modules-2.02-0.33.el7_2

RHEL7WS
x86_64
grub2-debuginfo-2.02-0.33.el7_2
grub2-tools-2.02-0.33.el7_2

grub2-2.02-0.33.el7_2
grub2-efi-2.02-0.33.el7_2
grub2-efi-modules-2.02-0.33.el7_2

144089 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2237-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:2237-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-December/001728.html

SuSE SLED 12
x86_64
libopenssl1_0_0-debuginfo-32bit-1.0.1i-27.6.1
libopenssl1_0_0-32bit-1.0.1i-27.6.1
openssl-debugsource-1.0.1i-27.6.1
openssl-1.0.1i-27.6.1
libopenssl1_0_0-debuginfo-1.0.1i-27.6.1
openssl-debuginfo-1.0.1i-27.6.1
libopenssl1_0_0-1.0.1i-27.6.1

SuSE SLES 12
noarch
openssl-doc-1.0.1i-27.6.1

x86_64
libopenssl1_0_0-debuginfo-32bit-1.0.1i-27.6.1
libopenssl1_0_0-32bit-1.0.1i-27.6.1
openssl-debugsource-1.0.1i-27.6.1
libopenssl1_0_0-hmac-32bit-1.0.1i-27.6.1
openssl-1.0.1i-27.6.1
libopenssl1_0_0-debuginfo-1.0.1i-27.6.1
openssl-debuginfo-1.0.1i-27.6.1
libopenssl1_0_0-1.0.1i-27.6.1
libopenssl1_0_0-hmac-1.0.1i-27.6.1

160008 - CentOS 7 CESA-2015-2653 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
CESA-2015-2653

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021545.html

CentOS 7
x86_64
grub2-efi-modules-2.02-0.33.el7.centos.1
grub2-efi-2.02-0.33.el7.centos.1
grub2-tools-2.02-0.33.el7.centos.1
grub2-2.02-0.33.el7.centos.1

160009 - CentOS 6, 7 CESA-2015-2617 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
CESA-2015-2617

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021524.html
http://lists.centos.org/pipermail/centos-announce/2015-December/021523.html
http://lists.centos.org/pipermail/centos-announce/2015-December/021519.html

CentOS 7
x86_64
openssl-static-1.0.1e-51.el7_2.1
openssl-devel-1.0.1e-51.el7_2.1
openssl-1.0.1e-51.el7_2.1
openssl-perl-1.0.1e-51.el7_2.1
openssl-libs-1.0.1e-51.el7_2.1

i686
openssl-static-1.0.1e-51.el7_2.1
openssl-devel-1.0.1e-51.el7_2.1
openssl-libs-1.0.1e-51.el7_2.1

CentOS 6
x86_64
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

i686
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

160010 - CentOS 5 CESA-2015-2616 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3195

Description

The scan detected that the host is missing the following update:
CESA-2015-2616

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-December/021520.html

CentOS 5
i386
openssl-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11

i686
openssl-0.9.8e-37.el5_11

x86_64
openssl-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11

170590 - Amazon Linux AMI ALAS-2015-624 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-5355, CVE-2015-2694

Description

The scan detected that the host is missing the following update:
ALAS-2015-624

Observation

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

https://alas.aws.amazon.com/ALAS-2015-624.html

Amazon Linux AMI
x86_64
krb5-debuginfo-1.13.2-10.39.amzn1
krb5-server-ldap-1.13.2-10.39.amzn1
krb5-workstation-1.13.2-10.39.amzn1
krb5-pkinit-openssl-1.13.2-10.39.amzn1
krb5-libs-1.13.2-10.39.amzn1
krb5-devel-1.13.2-10.39.amzn1
krb5-server-1.13.2-10.39.amzn1

i686
krb5-pkinit-openssl-1.13.2-10.39.amzn1

krb5-server-ldap-1.13.2-10.39.amzn1
krb5-workstation-1.13.2-10.39.amzn1
krb5-debuginfo-1.13.2-10.39.amzn1
krb5-libs-1.13.2-10.39.amzn1
krb5-devel-1.13.2-10.39.amzn1
krb5-server-1.13.2-10.39.amzn1

170596 - Amazon Linux AMI ALAS-2015-622 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2150

Description

The scan detected that the host is missing the following update:
ALAS-2015-622

Observation

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

https://alas.aws.amazon.com/ALAS-2015-622.html

Amazon Linux AMI
x86_64
xfsprogs-devel-3.2.2-2.20.amzn1
xfsprogs-debuginfo-3.2.2-2.20.amzn1
xfsprogs-3.2.2-2.20.amzn1

i686
xfsprogs-devel-3.2.2-2.20.amzn1
xfsprogs-debuginfo-3.2.2-2.20.amzn1
xfsprogs-3.2.2-2.20.amzn1

170602 - Amazon Linux AMI ALAS-2015-614 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
ALAS-2015-614

Observation

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

https://alas.aws.amazon.com/ALAS-2015-614.html

Amazon Linux AMI
x86_64
openssl-devel-1.0.1k-13.88.amzn1
openssl-1.0.1k-13.88.amzn1
openssl-debuginfo-1.0.1k-13.88.amzn1
openssl-static-1.0.1k-13.88.amzn1

openssl-perl-1.0.1k-13.88.amzn1

i686
openssl-devel-1.0.1k-13.88.amzn1
openssl-debuginfo-1.0.1k-13.88.amzn1
openssl-1.0.1k-13.88.amzn1
openssl-static-1.0.1k-13.88.amzn1
openssl-perl-1.0.1k-13.88.amzn1

170603 - Amazon Linux AMI ALAS-2015-615 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7981, CVE-2015-8472

Description

The scan detected that the host is missing the following update:
ALAS-2015-615

Observation

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

https://alas.aws.amazon.com/ALAS-2015-615.html

Amazon Linux AMI
x86_64
libpng-static-1.2.49-2.14.amzn1
libpng-debuginfo-1.2.49-2.14.amzn1
libpng-1.2.49-2.14.amzn1
libpng-devel-1.2.49-2.14.amzn1

i686
libpng-static-1.2.49-2.14.amzn1
libpng-debuginfo-1.2.49-2.14.amzn1
libpng-1.2.49-2.14.amzn1
libpng-devel-1.2.49-2.14.amzn1

170606 - Amazon Linux AMI ALAS-2015-613 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7545

Description

The scan detected that the host is missing the following update:
ALAS-2015-613

Observation

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

https://alas.aws.amazon.com/ALAS-2015-613.html

Amazon Linux AMI
i686

git-svn-2.4.3-7.42.amzn1
git-debuginfo-2.4.3-7.42.amzn1
git-2.4.3-7.42.amzn1
git-daemon-2.4.3-7.42.amzn1

noarch
git-email-2.4.3-7.42.amzn1
git-bzr-2.4.3-7.42.amzn1
gitweb-2.4.3-7.42.amzn1
perl-Git-2.4.3-7.42.amzn1
git-p4-2.4.3-7.42.amzn1
emacs-git-el-2.4.3-7.42.amzn1
emacs-git-2.4.3-7.42.amzn1
perl-Git-SVN-2.4.3-7.42.amzn1
git-hg-2.4.3-7.42.amzn1
git-cvs-2.4.3-7.42.amzn1
git-all-2.4.3-7.42.amzn1

x86_64
git-svn-2.4.3-7.42.amzn1
git-debuginfo-2.4.3-7.42.amzn1
git-2.4.3-7.42.amzn1
git-daemon-2.4.3-7.42.amzn1

174713 - Scientific Linux Security ERRATA Moderate: abrt on SL6.x i386/x86_64 (1507-5735)

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

Risk Level: Medium

CVE: CVE-2015-1869, CVE-2015-1870, CVE-2015-3142, CVE-2015-3147, CVE-2015-3159, CVE-2015-3315

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: abrt on SL6.x i386/x86_64 (1507-5735)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=5735

SL6
i386
libreport-plugin-bugzilla-2.0.9-21.el6_6.1
libreport-plugin-mailx-2.0.9-21.el6_6.1
abrt-2.0.8-26.el6_6.1
abrt-addon-ccpp-2.0.8-26.el6_6.1
libreport-2.0.9-21.el6_6.1
libreport-plugin-reportuploader-2.0.9-21.el6_6.1
abrt-addon-kerneloops-2.0.8-26.el6_6.1
libreport-newt-2.0.9-21.el6_6.1
libreport-plugin-rhtsupport-2.0.9-21.el6_6.1
abrt-addon-vmcore-2.0.8-26.el6_6.1
libreport-plugin-logger-2.0.9-21.el6_6.1
abrt-cli-2.0.8-26.el6_6.1
libreport-gtk-2.0.9-21.el6_6.1
abrt-tui-2.0.8-26.el6_6.1
abrt-debuginfo-2.0.8-26.el6_6.1
libreport-gtk-devel-2.0.9-21.el6_6.1

libreport-filesystem-2.0.9-21.el6_6.1
abrt-gui-2.0.8-26.el6_6.1
abrt-libs-2.0.8-26.el6_6.1
libreport-compat-2.0.9-21.el6_6.1
abrt-addon-python-2.0.8-26.el6_6.1
libreport-debuginfo-2.0.9-21.el6_6.1
libreport-cli-2.0.9-21.el6_6.1
abrt-desktop-2.0.8-26.el6_6.1
libreport-plugin-kerneloops-2.0.9-21.el6_6.1
libreport-python-2.0.9-21.el6_6.1
abrt-devel-2.0.8-26.el6_6.1
libreport-devel-2.0.9-21.el6_6.1
abrt-console-notification-2.0.8-26.el6_6.1

noarch
abrt-python-2.0.8-26.el6_6.1

x86_64
libreport-plugin-bugzilla-2.0.9-21.el6_6.1
libreport-plugin-mailx-2.0.9-21.el6_6.1
abrt-2.0.8-26.el6_6.1
abrt-addon-ccpp-2.0.8-26.el6_6.1
libreport-2.0.9-21.el6_6.1
libreport-plugin-reportuploader-2.0.9-21.el6_6.1
abrt-addon-kerneloops-2.0.8-26.el6_6.1
libreport-newt-2.0.9-21.el6_6.1
libreport-plugin-rhtsupport-2.0.9-21.el6_6.1
abrt-addon-vmcore-2.0.8-26.el6_6.1
libreport-plugin-logger-2.0.9-21.el6_6.1
abrt-cli-2.0.8-26.el6_6.1
libreport-gtk-2.0.9-21.el6_6.1
abrt-tui-2.0.8-26.el6_6.1
abrt-debuginfo-2.0.8-26.el6_6.1
libreport-gtk-devel-2.0.9-21.el6_6.1
libreport-filesystem-2.0.9-21.el6_6.1
abrt-gui-2.0.8-26.el6_6.1
abrt-libs-2.0.8-26.el6_6.1
libreport-compat-2.0.9-21.el6_6.1
abrt-addon-python-2.0.8-26.el6_6.1
libreport-debuginfo-2.0.9-21.el6_6.1
libreport-cli-2.0.9-21.el6_6.1
abrt-desktop-2.0.8-26.el6_6.1
libreport-plugin-kerneloops-2.0.9-21.el6_6.1
libreport-python-2.0.9-21.el6_6.1
abrt-devel-2.0.8-26.el6_6.1
libreport-devel-2.0.9-21.el6_6.1
abrt-console-notification-2.0.8-26.el6_6.1

174714 - Scientific Linux Security ERRATA Moderate: openssl on SL6.x i386/x86_64 (1512-1245)

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssl on SL6.x i386/x86_64 (1512-1245)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=1245

SL6
x86_64
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

i386
openssl-debuginfo-1.0.1e-42.el6_7.1
openssl-static-1.0.1e-42.el6_7.1
openssl-1.0.1e-42.el6_7.1
openssl-perl-1.0.1e-42.el6_7.1
openssl-devel-1.0.1e-42.el6_7.1

174721 - Scientific Linux Security ERRATA Moderate: subversion on SL7.x x86_64 (1509-10618)

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

Risk Level: Medium

CVE: CVE-2015-0248, CVE-2015-0251, CVE-2015-3184, CVE-2015-3187

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: subversion on SL7.x x86_64 (1509-10618)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=10618

SL7
x86_64
subversion-perl-1.7.14-7.el7_1.1
subversion-javahl-1.7.14-7.el7_1.1
subversion-tools-1.7.14-7.el7_1.1
subversion-kde-1.7.14-7.el7_1.1
subversion-ruby-1.7.14-7.el7_1.1
mod_dav_svn-1.7.14-7.el7_1.1
subversion-python-1.7.14-7.el7_1.1
subversion-devel-1.7.14-7.el7_1.1
subversion-1.7.14-7.el7_1.1
subversion-libs-1.7.14-7.el7_1.1
subversion-debuginfo-1.7.14-7.el7_1.1
subversion-gnome-1.7.14-7.el7_1.1

174724 - Scientific Linux Security ERRATA Moderate: openssl on SL5.x i386/x86_64 (1512-919)

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

Risk Level: Medium

CVE: CVE-2015-3195

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssl on SL5.x i386/x86_64 (1512-919)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1512&L=scientific-linux-errata&F=&S=&P=919

SL5
x86_64
openssl-debuginfo-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

i386
openssl-debuginfo-0.9.8e-37.el5_11
openssl-devel-0.9.8e-37.el5_11
openssl-perl-0.9.8e-37.el5_11
openssl-0.9.8e-37.el5_11

174730 - Scientific Linux Security ERRATA Low: httpd on SL6.x i386/x86_64 (1508-7627)

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

Risk Level: Medium

CVE: CVE-2013-5704

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: httpd on SL6.x i386/x86_64 (1508-7627)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=7627

SL6
i386
httpd-devel-2.2.15-45.sl6
httpd-2.2.15-45.sl6
httpd-debuginfo-2.2.15-45.sl6
httpd-tools-2.2.15-45.sl6
mod_ssl-2.2.15-45.sl6

noarch
httpd-manual-2.2.15-45.sl6

x86_64
httpd-devel-2.2.15-45.sl6
httpd-2.2.15-45.sl6
httpd-debuginfo-2.2.15-45.sl6
httpd-tools-2.2.15-45.sl6
mod_ssl-2.2.15-45.sl6

174734 - Scientific Linux Security ERRATA Moderate: httpd on SL6.x i386/x86_64 (1508-22101)

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

Risk Level: Medium

CVE: CVE-2015-3183

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: httpd on SL6.x i386/x86_64 (1508-22101)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=22101

SL6
i386
mod_ssl-2.2.15-47.sl6
httpd-debuginfo-2.2.15-47.sl6
httpd-tools-2.2.15-47.sl6
httpd-devel-2.2.15-47.sl6
httpd-2.2.15-47.sl6

noarch
httpd-manual-2.2.15-47.sl6

x86_64
mod_ssl-2.2.15-47.sl6
httpd-debuginfo-2.2.15-47.sl6
httpd-tools-2.2.15-47.sl6
httpd-devel-2.2.15-47.sl6
httpd-2.2.15-47.sl6

174742 - Scientific Linux Security ERRATA Moderate: gnutls on SL6.x i386/x86_64 (1508-1412)

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

Risk Level: Medium

CVE: CVE-2014-8155, CVE-2015-0282, CVE-2015-0294

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: gnutls on SL6.x i386/x86_64 (1508-1412)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=1412

SL6
x86_64
gnutls-utils-2.8.5-18.el6
gnutls-debuginfo-2.8.5-18.el6
gnutls-devel-2.8.5-18.el6

gnutls-2.8.5-18.el6
gnutls-guile-2.8.5-18.el6

i386
gnutls-utils-2.8.5-18.el6
gnutls-debuginfo-2.8.5-18.el6
gnutls-devel-2.8.5-18.el6
gnutls-2.8.5-18.el6
gnutls-guile-2.8.5-18.el6

174750 - Scientific Linux Security ERRATA Moderate: xerces-c on SL7.x x86_64 (1506-14887)

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

Risk Level: Medium

CVE: CVE-2015-0252

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: xerces-c on SL7.x x86_64 (1506-14887)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=14887

SL7
x86_64
xerces-c-devel-3.1.1-7.el7_1
xerces-c-3.1.1-7.el7_1
xerces-c-debuginfo-3.1.1-7.el7_1

noarch
xerces-c-doc-3.1.1-7.el7_1

174760 - Scientific Linux Security ERRATA Important: wpa_supplicant on SL7.x x86_64 (1506-6623)

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

Risk Level: Medium

CVE: CVE-2015-1863, CVE-2015-4142

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: wpa_supplicant on SL7.x x86_64 (1506-6623)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=6623

SL7
x86_64
wpa_supplicant-2.0-17.el7_1
wpa_supplicant-debuginfo-2.0-17.el7_1

174765 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1509-15659)

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

Risk Level: Medium

CVE: CVE-2015-5165

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1509-15659)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=15659

SL7
x86_64
qemu-kvm-tools-1.5.3-86.el7_1.6
libcacard-devel-1.5.3-86.el7_1.6
qemu-img-1.5.3-86.el7_1.6
qemu-kvm-debuginfo-1.5.3-86.el7_1.6
qemu-kvm-1.5.3-86.el7_1.6
libcacard-tools-1.5.3-86.el7_1.6
libcacard-1.5.3-86.el7_1.6
qemu-kvm-common-1.5.3-86.el7_1.6

174767 - Scientific Linux Security ERRATA Moderate: sudo on SL6.x i386/x86_64 (1508-2462)

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

Risk Level: Medium

CVE: CVE-2014-9680

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: sudo on SL6.x i386/x86_64 (1508-2462)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=2462

SL6
x86_64
sudo-debuginfo-1.8.6p3-19.el6
sudo-1.8.6p3-19.el6
sudo-devel-1.8.6p3-19.el6

i386
sudo-debuginfo-1.8.6p3-19.el6
sudo-1.8.6p3-19.el6
sudo-devel-1.8.6p3-19.el6

174769 - Scientific Linux Security ERRATA Moderate: libreport on SL6.x i386/x86_64 (1511-16326)

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

Risk Level: Medium

CVE: CVE-2015-5302

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreport on SL6.x i386/x86_64 (1511-16326)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=16326

SL6
x86_64
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

i386
libreport-plugin-logger-2.0.9-25.el6_7
libreport-newt-2.0.9-25.el6_7
libreport-compat-2.0.9-25.el6_7
libreport-python-2.0.9-25.el6_7
libreport-debuginfo-2.0.9-25.el6_7
libreport-gtk-2.0.9-25.el6_7
libreport-cli-2.0.9-25.el6_7
libreport-2.0.9-25.el6_7
libreport-plugin-bugzilla-2.0.9-25.el6_7
libreport-filesystem-2.0.9-25.el6_7
libreport-plugin-mailx-2.0.9-25.el6_7
libreport-plugin-rhtsupport-2.0.9-25.el6_7
libreport-plugin-kerneloops-2.0.9-25.el6_7
libreport-devel-2.0.9-25.el6_7
libreport-gtk-devel-2.0.9-25.el6_7
libreport-plugin-ureport-2.0.9-25.el6_7
libreport-plugin-reportuploader-2.0.9-25.el6_7

174771 - Scientific Linux Security ERRATA Moderate: openssl on SL5.x i386/x86_64 (1506-15584)

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

Risk Level: Medium

CVE: CVE-2015-1789, CVE-2015-1790, CVE-2015-4000

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssl on SL5.x i386/x86_64 (1506-15584)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=15584

SL5
x86_64
openssl-0.9.8e-36.el5_11
openssl-debuginfo-0.9.8e-36.el5_11
openssl-perl-0.9.8e-36.el5_11
openssl-devel-0.9.8e-36.el5_11

i386
openssl-0.9.8e-36.el5_11
openssl-debuginfo-0.9.8e-36.el5_11
openssl-perl-0.9.8e-36.el5_11
openssl-devel-0.9.8e-36.el5_11

174773 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1510-6479)

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

Risk Level: Medium

CVE: CVE-2015-1779

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL7.x x86_64 (1510-6479)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=6479

SL7
x86_64
libcacard-tools-1.5.3-86.el7_1.8
qemu-img-1.5.3-86.el7_1.8
qemu-kvm-common-1.5.3-86.el7_1.8
qemu-kvm-1.5.3-86.el7_1.8
qemu-kvm-debuginfo-1.5.3-86.el7_1.8
qemu-kvm-tools-1.5.3-86.el7_1.8
libcacard-1.5.3-86.el7_1.8
libcacard-devel-1.5.3-86.el7_1.8

174775 - Scientific Linux Security ERRATA Moderate: mariadb on SL7.x x86_64 (1508-22767)

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

Risk Level: Medium

CVE: CVE-2015-0433, CVE-2015-0441, CVE-2015-0499, CVE-2015-0501, CVE-2015-0505, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2582, CVE-2015-2620, CVE-2015-2643, CVE-2015-2648, CVE-2015-3152, CVE-2015-4737, CVE-2015-4752, CVE-2015-4757

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: mariadb on SL7.x x86_64 (1508-22767)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=22767

SL7
x86_64
mariadb-test-5.5.44-1.el7_1
mariadb-embedded-5.5.44-1.el7_1
mariadb-embedded-devel-5.5.44-1.el7_1
mariadb-devel-5.5.44-1.el7_1
mariadb-server-5.5.44-1.el7_1
mariadb-5.5.44-1.el7_1
mariadb-libs-5.5.44-1.el7_1
mariadb-bench-5.5.44-1.el7_1
mariadb-debuginfo-5.5.44-1.el7_1

174791 - Scientific Linux Security ERRATA Important: openldap on SL5.x, SL6.x, SL7.x i386/x86_64 (1509-21602)

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

Risk Level: Medium

CVE: CVE-2015-6908

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: openldap on SL5.x, SL6.x, SL7.x i386/x86_64 (1509-21602)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=21602

SL5
x86_64
compat-openldap-2.3.43_2.2.29-29.el5_11
openldap-clients-2.3.43-29.el5_11
openldap-debuginfo-2.3.43-29.el5_11
openldap-servers-overlays-2.3.43-29.el5_11
openldap-servers-2.3.43-29.el5_11
openldap-devel-2.3.43-29.el5_11
openldap-2.3.43-29.el5_11
openldap-servers-sql-2.3.43-29.el5_11

i386
compat-openldap-2.3.43_2.2.29-29.el5_11
openldap-clients-2.3.43-29.el5_11
openldap-debuginfo-2.3.43-29.el5_11

openldap-servers-overlays-2.3.43-29.el5_11
openldap-servers-2.3.43-29.el5_11
openldap-devel-2.3.43-29.el5_11
openldap-2.3.43-29.el5_11
openldap-servers-sql-2.3.43-29.el5_11

SL7
x86_64
openldap-servers-sql-2.4.39-7.el7_1
openldap-2.4.39-7.el7_1
openldap-devel-2.4.39-7.el7_1
openldap-clients-2.4.39-7.el7_1
openldap-servers-2.4.39-7.el7_1
openldap-debuginfo-2.4.39-7.el7_1

SL6
x86_64
openldap-clients-2.4.40-6.el6_7
openldap-devel-2.4.40-6.el6_7
openldap-servers-sql-2.4.40-6.el6_7
openldap-2.4.40-6.el6_7
openldap-servers-2.4.40-6.el6_7
openldap-debuginfo-2.4.40-6.el6_7

i386
openldap-clients-2.4.40-6.el6_7
openldap-devel-2.4.40-6.el6_7
openldap-servers-sql-2.4.40-6.el6_7
openldap-2.4.40-6.el6_7
openldap-servers-2.4.40-6.el6_7
openldap-debuginfo-2.4.40-6.el6_7

174793 - Scientific Linux Security ERRATA Moderate: libreswan on SL7.x x86_64 (1506-12300)

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

Risk Level: Medium

CVE: CVE-2015-3204

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreswan on SL7.x x86_64 (1506-12300)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=12300

SL7
x86_64
libreswan-debuginfo-3.12-10.1.el7_1
libreswan-3.12-10.1.el7_1

174797 - Scientific Linux Security ERRATA Moderate: wireshark on SL6.x i386/x86_64 (1508-4657)

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

Risk Level: Medium

CVE: CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714, CVE-2015-0562, CVE-2015-0564, CVE-2015-2189, CVE-2015-2191

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wireshark on SL6.x i386/x86_64 (1508-4657)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=4657

SL6
x86_64
wireshark-gnome-1.8.10-17.el6
wireshark-1.8.10-17.el6
wireshark-devel-1.8.10-17.el6
wireshark-debuginfo-1.8.10-17.el6

i386
wireshark-gnome-1.8.10-17.el6
wireshark-1.8.10-17.el6
wireshark-devel-1.8.10-17.el6
wireshark-debuginfo-1.8.10-17.el6

174800 - Scientific Linux Security ERRATA Moderate: glibc on SL5.x i386/x86_64 (1508-16270)

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

Risk Level: Medium

CVE: CVE-2013-7424

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: glibc on SL5.x i386/x86_64 (1508-16270)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=16270

SL5
x86_64
glibc-devel-2.5-123.el5_11.3
nscd-2.5-123.el5_11.3
glibc-2.5-123.el5_11.3
glibc-debuginfo-2.5-123.el5_11.3
glibc-headers-2.5-123.el5_11.3
glibc-common-2.5-123.el5_11.3
glibc-debuginfo-common-2.5-123.el5_11.3
glibc-utils-2.5-123.el5_11.3

i386
glibc-devel-2.5-123.el5_11.3
nscd-2.5-123.el5_11.3
glibc-2.5-123.el5_11.3

glibc-debuginfo-2.5-123.el5_11.3
glibc-headers-2.5-123.el5_11.3
glibc-common-2.5-123.el5_11.3
glibc-debuginfo-common-2.5-123.el5_11.3
glibc-utils-2.5-123.el5_11.3

174801 - Scientific Linux Security ERRATA Moderate: httpd on SL7.x x86_64 (1508-22428)

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

Risk Level: Medium

CVE: CVE-2015-3183, CVE-2015-3185

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: httpd on SL7.x x86_64 (1508-22428)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=22428

SL7
x86_64
httpd-debuginfo-2.4.6-31.sl7.1
mod_ssl-2.4.6-31.sl7.1
mod_session-2.4.6-31.sl7.1
mod_ldap-2.4.6-31.sl7.1
httpd-devel-2.4.6-31.sl7.1
httpd-tools-2.4.6-31.sl7.1
mod_proxy_html-2.4.6-31.sl7.1
httpd-2.4.6-31.sl7.1

noarch
httpd-manual-2.4.6-31.sl7.1

174802 - Scientific Linux Security ERRATA Critical: openafs on SL5.x, SL6.x, SL7.x i386/x86_64 (1510-6806)

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

Risk Level: Medium

CVE: CVE-2015-7762, CVE-2015-7763

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: openafs on SL5.x, SL6.x, SL7.x i386/x86_64 (1510-6806)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1510&L=scientific-linux-errata&F=&S=&P=6806

SL5
x86_64
openafs-authlibs-1.4.15-88.sl5
openafs-devel-1.4.15-88.sl5

kernel-module-openafs-2.6.18-406.el5xen-1.4.15-88.sl5
openafs-kernel-source-1.4.15-88.sl5
openafs-server-1.4.15-88.sl5
openafs-compat-1.4.15-88.sl5
openafs-client-1.4.15-88.sl5
openafs-krb5-1.4.15-88.sl5
openafs-debug-1.4.15-88.sl5
openafs-1.4.15-88.sl5
kernel-module-openafs-2.6.18-406.el5-1.4.15-88.sl5
openafs-authlibs-devel-1.4.15-88.sl5
openafs-kpasswd-1.4.15-88.sl5

i386
openafs-authlibs-1.4.15-88.sl5
openafs-devel-1.4.15-88.sl5
kernel-module-openafs-2.6.18-406.el5xen-1.4.15-88.sl5
openafs-kernel-source-1.4.15-88.sl5
openafs-server-1.4.15-88.sl5
openafs-compat-1.4.15-88.sl5
openafs-krb5-1.4.15-88.sl5
openafs-client-1.4.15-88.sl5
openafs-debug-1.4.15-88.sl5
kernel-module-openafs-2.6.18-406.el5PAE-1.4.15-88.sl5
openafs-1.4.15-88.sl5
kernel-module-openafs-2.6.18-406.el5-1.4.15-88.sl5
openafs-authlibs-devel-1.4.15-88.sl5
openafs-kpasswd-1.4.15-88.sl5

SL7
x86_64
kmod-openafs-1.6-sl-229-1.6.14-219.sl7.229.14.1
openafs-1.6-sl-authlibs-1.6.14-219.sl7
openafs-1.6-sl-devel-1.6.14-219.sl7
openafs-1.6-sl-server-1.6.14-219.sl7
openafs-1.6-sl-krb5-1.6.14-219.sl7
openafs-1.6-sl-client-1.6.14-219.sl7
openafs-1.6-sl-module-tools-1.6.14-219.sl7
openafs-1.6-sl-compat-1.6.14-219.sl7
openafs-1.6-sl-kernel-source-1.6.14-219.sl7
openafs-1.6-sl-plumbing-tools-1.6.14-219.sl7
openafs-1.6-sl-1.6.14-219.sl7
openafs-1.6-sl-kpasswd-1.6.14-219.sl7
openafs-1.6-sl-authlibs-devel-1.6.14-219.sl7

SL6
x86_64
kmod-openafs-573-1.6.14-219.sl6.573.3.1
openafs-devel-1.6.14-219.sl6
openafs-kernel-source-1.6.14-219.sl6
openafs-compat-1.6.14-219.sl6
openafs-module-tools-1.6.14-219.sl6
openafs-plumbing-tools-1.6.14-219.sl6
openafs-1.6.14-219.sl6
openafs-kpasswd-1.6.14-219.sl6
openafs-server-1.6.14-219.sl6
openafs-client-1.6.14-219.sl6
openafs-authlibs-devel-1.6.14-219.sl6
openafs-authlibs-1.6.14-219.sl6
openafs-krb5-1.6.14-219.sl6

i386
kmod-openafs-573-1.6.14-219.sl6.573.3.1
openafs-devel-1.6.14-219.sl6
openafs-kernel-source-1.6.14-219.sl6
openafs-compat-1.6.14-219.sl6
openafs-module-tools-1.6.14-219.sl6
openafs-plumbing-tools-1.6.14-219.sl6
openafs-1.6.14-219.sl6
openafs-kpasswd-1.6.14-219.sl6
openafs-server-1.6.14-219.sl6
openafs-client-1.6.14-219.sl6
openafs-authlibs-devel-1.6.14-219.sl6
openafs-authlibs-1.6.14-219.sl6
openafs-krb5-1.6.14-219.sl6

174804 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1507-7426)

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

Risk Level: Medium

CVE: CVE-2011-5321, CVE-2015-1593, CVE-2015-2830, CVE-2015-2922, CVE-2015-3636

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: kernel on SL6.x i386/x86_64 (1507-7426)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1507&L=scientific-linux-errata&F=&S=&P=7426

SL6
i386
python-perf-2.6.32-504.30.3.el6
perf-2.6.32-504.30.3.el6
kernel-2.6.32-504.30.3.el6
kernel-debuginfo-common-i686-2.6.32-504.30.3.el6
kernel-debug-debuginfo-2.6.32-504.30.3.el6
kernel-debug-2.6.32-504.30.3.el6
kernel-headers-2.6.32-504.30.3.el6
kernel-debuginfo-2.6.32-504.30.3.el6
kernel-devel-2.6.32-504.30.3.el6
python-perf-debuginfo-2.6.32-504.30.3.el6
perf-debuginfo-2.6.32-504.30.3.el6
kernel-debug-devel-2.6.32-504.30.3.el6

noarch
dracut-fips-aesni-004-356.el6_6.3
dracut-004-356.el6_6.3
dracut-caps-004-356.el6_6.3
dracut-kernel-004-356.el6_6.3
kernel-doc-2.6.32-504.30.3.el6
dracut-tools-004-356.el6_6.3
dracut-network-004-356.el6_6.3
dracut-fips-004-356.el6_6.3
kernel-firmware-2.6.32-504.30.3.el6
dracut-generic-004-356.el6_6.3
kernel-abi-whitelists-2.6.32-504.30.3.el6

x86_64
perf-2.6.32-504.30.3.el6
kernel-2.6.32-504.30.3.el6
kernel-headers-2.6.32-504.30.3.el6
kernel-debug-debuginfo-2.6.32-504.30.3.el6
kernel-debug-2.6.32-504.30.3.el6
python-perf-2.6.32-504.30.3.el6
kernel-debuginfo-2.6.32-504.30.3.el6
kernel-devel-2.6.32-504.30.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.30.3.el6
python-perf-debuginfo-2.6.32-504.30.3.el6
perf-debuginfo-2.6.32-504.30.3.el6
kernel-debug-devel-2.6.32-504.30.3.el6

174806 - Scientific Linux Security ERRATA Moderate: subversion on SL6.x i386/x86_64 (1508-15573)

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

Risk Level: Medium

CVE: CVE-2015-0248, CVE-2015-0251, CVE-2015-3187

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: subversion on SL6.x i386/x86_64 (1508-15573)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=15573

SL6
i386
mod_dav_svn-1.6.11-15.el6_7
subversion-perl-1.6.11-15.el6_7
subversion-kde-1.6.11-15.el6_7
subversion-debuginfo-1.6.11-15.el6_7
subversion-javahl-1.6.11-15.el6_7
subversion-devel-1.6.11-15.el6_7
subversion-gnome-1.6.11-15.el6_7
subversion-1.6.11-15.el6_7
subversion-ruby-1.6.11-15.el6_7

noarch
subversion-svn2cl-1.6.11-15.el6_7

x86_64
mod_dav_svn-1.6.11-15.el6_7
subversion-perl-1.6.11-15.el6_7
subversion-kde-1.6.11-15.el6_7
subversion-debuginfo-1.6.11-15.el6_7
subversion-javahl-1.6.11-15.el6_7
subversion-devel-1.6.11-15.el6_7
subversion-gnome-1.6.11-15.el6_7
subversion-1.6.11-15.el6_7
subversion-ruby-1.6.11-15.el6_7

174813 - Scientific Linux Security ERRATA Low: libxml2 on SL6.x i386/x86_64 (1508-2135)

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

Risk Level: Medium

CVE: CVE-2015-1819

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: libxml2 on SL6.x i386/x86_64 (1508-2135)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=2135

SL6
x86_64
libxml2-static-2.7.6-20.el6
libxml2-debuginfo-2.7.6-20.el6
libxml2-2.7.6-20.el6
libxml2-python-2.7.6-20.el6
libxml2-devel-2.7.6-20.el6

i386
libxml2-static-2.7.6-20.el6
libxml2-debuginfo-2.7.6-20.el6
libxml2-2.7.6-20.el6
libxml2-python-2.7.6-20.el6
libxml2-devel-2.7.6-20.el6

174821 - Scientific Linux Security ERRATA Moderate: pam on SL6.x, SL7.x i386/x86_64 (1508-21406)

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

Risk Level: Medium

CVE: CVE-2015-3238

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pam on SL6.x, SL7.x i386/x86_64 (1508-21406)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=21406

SL7
x86_64
pam-debuginfo-1.1.8-12.el7_1.1
pam-1.1.8-12.el7_1.1
pam-devel-1.1.8-12.el7_1.1

SL6
x86_64
pam-1.1.1-20.el6_7.1
pam-debuginfo-1.1.1-20.el6_7.1
pam-devel-1.1.1-20.el6_7.1

i386
pam-1.1.1-20.el6_7.1
pam-debuginfo-1.1.1-20.el6_7.1
pam-devel-1.1.1-20.el6_7.1

174822 - Scientific Linux Security ERRATA Important: haproxy on SL6.x, SL7.x i386/x86_64 (1509-10281)

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

Risk Level: Medium

CVE: CVE-2015-3281

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: haproxy on SL6.x, SL7.x i386/x86_64 (1509-10281)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=10281

SL7
x86_64
haproxy-1.5.4-4.el7_1.1
haproxy-debuginfo-1.5.4-4.el7_1.1

SL6
x86_64
haproxy-1.5.4-2.el6_7.1
haproxy-debuginfo-1.5.4-2.el6_7.1

i386
haproxy-1.5.4-2.el6_7.1
haproxy-debuginfo-1.5.4-2.el6_7.1

174823 - Scientific Linux Security ERRATA Moderate: curl on SL6.x i386/x86_64 (1508-7212)

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

Risk Level: Medium

CVE: CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL6.x i386/x86_64 (1508-7212)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=7212

SL6
x86_64
curl-debuginfo-7.19.7-46.el6
curl-7.19.7-46.el6

libcurl-devel-7.19.7-46.el6
libcurl-7.19.7-46.el6

i386
curl-debuginfo-7.19.7-46.el6
curl-7.19.7-46.el6
libcurl-devel-7.19.7-46.el6
libcurl-7.19.7-46.el6

174824 - Scientific Linux Security ERRATA Moderate: net-snmp on SL6.x i386/x86_64 (1508-5847)

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

Risk Level: Medium

CVE: CVE-2014-3565

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: net-snmp on SL6.x i386/x86_64 (1508-5847)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=5847

SL6
x86_64
net-snmp-devel-5.5-54.el6
net-snmp-perl-5.5-54.el6
net-snmp-libs-5.5-54.el6
net-snmp-utils-5.5-54.el6
net-snmp-python-5.5-54.el6
net-snmp-5.5-54.el6
net-snmp-debuginfo-5.5-54.el6

i386
net-snmp-devel-5.5-54.el6
net-snmp-perl-5.5-54.el6
net-snmp-libs-5.5-54.el6
net-snmp-utils-5.5-54.el6
net-snmp-python-5.5-54.el6
net-snmp-5.5-54.el6
net-snmp-debuginfo-5.5-54.el6

174828 - Scientific Linux Security ERRATA Moderate: qemu-kvm on SL6.x i386/x86_64 (1509-16429)

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

Risk Level: Medium

CVE: CVE-2015-5165

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: qemu-kvm on SL6.x i386/x86_64 (1509-16429)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=16429

SL6
x86_64
qemu-kvm-tools-0.12.1.2-2.479.el6_7.1
qemu-guest-agent-0.12.1.2-2.479.el6_7.1
qemu-img-0.12.1.2-2.479.el6_7.1
qemu-kvm-0.12.1.2-2.479.el6_7.1
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.1

i386
qemu-kvm-debuginfo-0.12.1.2-2.479.el6_7.1
qemu-guest-agent-0.12.1.2-2.479.el6_7.1

178073 - Gentoo Linux GLSA-201507-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0841

Description

The scan detected that the host is missing the following update:
GLSA-201507-12

Observation

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

https://security.gentoo.org/glsa/201507-12

Affected packages:
net-libs/libcapsinetwork <= 0.3.0-r2

178077 - Gentoo Linux GLSA-201509-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9390

Description

The scan detected that the host is missing the following update:
GLSA-201509-06

Observation

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

https://security.gentoo.org/glsa/201509-06

Affected packages:
dev-vcs/git < 2.0.5

178079 - Gentoo Linux GLSA-201507-17 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3565

Description

The scan detected that the host is missing the following update:
GLSA-201507-17

Observation

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

https://security.gentoo.org/glsa/201507-17

Affected packages:
net-analyzer/net-snmp < 5.7.3_pre5-r1

178095 - Gentoo Linux GLSA-201508-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3026

Description

The scan detected that the host is missing the following update:
GLSA-201508-03

Observation

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

https://security.gentoo.org/glsa/201508-03

Affected packages:
net-misc/icecast < 2.4.2

178096 - Gentoo Linux GLSA-201504-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9680

Description

The scan detected that the host is missing the following update:
GLSA-201504-02

Observation

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

https://security.gentoo.org/glsa/201504-02

Affected packages:
app-admin/sudo < 1.8.12

178105 - Gentoo Linux GLSA-201507-19 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0405, CVE-2015-0423, CVE-2015-0433, CVE-2015-0438, CVE-2015-0439, CVE-2015-0441, CVE-2015-0498, CVE-2015-0499, CVE-2015-0500, CVE-2015-0501, CVE-2015-0503, CVE-2015-0505, CVE-2015-0506, CVE-2015-0507, CVE-2015-0508, CVE-2015-0511, CVE-2015-2566, CVE-2015-2567, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573

Description

The scan detected that the host is missing the following update:
GLSA-201507-19

Observation

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

https://security.gentoo.org/glsa/201507-19

Affected packages:
dev-db/mysql < 5.6.24

178107 - Gentoo Linux GLSA-201507-18 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1266, CVE-2015-1267, CVE-2015-1268, CVE-2015-1269

Description

The scan detected that the host is missing the following update:
GLSA-201507-18

Observation

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

https://security.gentoo.org/glsa/201507-18

Affected packages:
www-client/chromium < 43.0.2357.130

178108 - Gentoo Linux GLSA-201507-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1819

Description

The scan detected that the host is missing the following update:
GLSA-201507-08

Observation

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

https://security.gentoo.org/glsa/201507-08

Affected packages:
dev-libs/libxml2 < 2.9.2-r1

178117 - Gentoo Linux GLSA-201511-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201511-01

Observation

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

https://security.gentoo.org/glsa/201511-01

Affected packages:
app-shells/mksh < 50c

178118 - Gentoo Linux GLSA-201507-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9449

Description

The scan detected that the host is missing the following update:
GLSA-201507-03

Observation

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

https://security.gentoo.org/glsa/201507-03

Affected packages:
media-gfx/exiv2 < 0.24-r1

178120 - Gentoo Linux GLSA-201503-13 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4607, CVE-2014-9645

Description

The scan detected that the host is missing the following update:
GLSA-201503-13

Observation

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

https://security.gentoo.org/glsa/201503-13

Affected packages:
sys-apps/busybox < 1.23.1

178126 - Gentoo Linux GLSA-201503-08 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-2270, CVE-2014-9620, CVE-2014-9621

Description

The scan detected that the host is missing the following update:
GLSA-201503-08

Observation

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

https://security.gentoo.org/glsa/201503-08

Affected packages:
sys-apps/file < 5.22

178130 - Gentoo Linux GLSA-201507-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2928, CVE-2015-2929

Description

The scan detected that the host is missing the following update:
GLSA-201507-02

Observation

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

https://security.gentoo.org/glsa/201507-02

Affected packages:
net-misc/tor < 0.2.6.7

181704 - FreeBSD redmine Open Redirect Vulnerability (c2efcd46-9ed5-11e5-8f5c-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2014-1985

Description

The scan detected that the host is missing the following update:
redmine -- open redirect vulnerability (c2efcd46-9ed5-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/c2efcd46-9ed5-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 2.4.5
redmine == 2.5.0

181705 - FreeBSD bind Multiple Vulnerabilities (a8ec4db7-a398-11e5-85e9-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2015-3193, CVE-2015-8000, CVE-2015-8461

Description

The scan detected that the host is missing the following update:
bind -- multiple vulnerabilities (a8ec4db7-a398-11e5-85e9-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/a8ec4db7-a398-11e5-85e9-14dae9d210b8.html

Affected packages:
bind99 < 9.9.8P2
bind910 < 9.10.3P2
bind9-devel < 9.11.0.a20151215

181717 - FreeBSD freeimage Multiple Integer Overflows (33459061-a1d6-11e5-8794-bcaec565249c)

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

Risk Level: Medium

CVE: CVE-2015-0852

Description

The scan detected that the host is missing the following update:
freeimage -- multiple integer overflows (33459061-a1d6-11e5-8794-bcaec565249c)

Observation

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

http://www.vuxml.org/freebsd/33459061-a1d6-11e5-8794-bcaec565249c.html

Affected packages:
freeimage < 3.16.0_1

190101 - Fedora Linux 22 FEDORA-2015-d87d60b9a9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d87d60b9a9

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173801.html

Fedora Core 22

openssl-1.0.1k-13.fc22

91979 - Oracle Enterprise Linux ELSA-2015-3107 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
ELSA-2015-3107

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-December/005620.html
http://oss.oracle.com/pipermail/el-errata/2015-December/005621.html

OEL7
x86_64
kernel-uek-debug-3.8.13-118.2.2.el7uek
kernel-uek-3.8.13-118.2.2.el7uek
kernel-uek-doc-3.8.13-118.2.2.el7uek
dtrace-modules-3.8.13-118.2.2.el7uek-0.4.5-3.el7
kernel-uek-debug-devel-3.8.13-118.2.2.el7uek
kernel-uek-devel-3.8.13-118.2.2.el7uek
kernel-uek-firmware-3.8.13-118.2.2.el7uek

OEL6
x86_64
kernel-uek-doc-3.8.13-118.2.2.el6uek
kernel-uek-3.8.13-118.2.2.el6uek
kernel-uek-devel-3.8.13-118.2.2.el6uek
kernel-uek-firmware-3.8.13-118.2.2.el6uek
kernel-uek-debug-devel-3.8.13-118.2.2.el6uek
dtrace-modules-3.8.13-118.2.2.el6uek-0.4.5-3.el6
kernel-uek-debug-3.8.13-118.2.2.el6uek

132203 - Oracle VM OVMSA-2015-0154 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0154

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-December/000402.html

OVM3.3
x86_64
kernel-uek-3.8.13-118.2.2.el6uek
kernel-uek-firmware-3.8.13-118.2.2.el6uek

144085 - SuSE Linux 13.1 openSUSE-SU-2015:2246-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4807, CVE-2015-4815, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4913

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2246-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00050.html

SuSE Linux 13.1
x86_64
libmysqlclient18-debuginfo-5.5.46-13.1
mariadb-debuginfo-5.5.46-13.1
mariadb-tools-debuginfo-5.5.46-13.1
libmysqlclient_r18-32bit-5.5.46-13.1
libmysqlclient_r18-5.5.46-13.1
libmysqlclient18-5.5.46-13.1
libmysqlclient18-32bit-5.5.46-13.1
mariadb-test-debuginfo-5.5.46-13.1
mariadb-errormessages-5.5.46-13.1
mariadb-debugsource-5.5.46-13.1
mariadb-client-5.5.46-13.1
mariadb-client-debuginfo-5.5.46-13.1
mariadb-5.5.46-13.1
libmysqlclient-devel-5.5.46-13.1
libmysqld18-debuginfo-5.5.46-13.1
libmysqld18-5.5.46-13.1
mariadb-tools-5.5.46-13.1

mariadb-bench-5.5.46-13.1
libmysqlclient18-debuginfo-32bit-5.5.46-13.1
libmysqld-devel-5.5.46-13.1
mariadb-test-5.5.46-13.1
mariadb-bench-debuginfo-5.5.46-13.1

i586
libmysqlclient18-debuginfo-5.5.46-13.1
mariadb-debuginfo-5.5.46-13.1
mariadb-tools-debuginfo-5.5.46-13.1
libmysqlclient_r18-5.5.46-13.1
libmysqlclient18-5.5.46-13.1
mariadb-test-debuginfo-5.5.46-13.1
mariadb-errormessages-5.5.46-13.1
mariadb-debugsource-5.5.46-13.1
mariadb-client-5.5.46-13.1
mariadb-client-debuginfo-5.5.46-13.1
mariadb-5.5.46-13.1
libmysqlclient-devel-5.5.46-13.1
libmysqld18-debuginfo-5.5.46-13.1
libmysqld18-5.5.46-13.1
mariadb-tools-5.5.46-13.1
mariadb-bench-5.5.46-13.1
libmysqld-devel-5.5.46-13.1
mariadb-test-5.5.46-13.1
mariadb-bench-debuginfo-5.5.46-13.1

144093 - SuSE Linux 13.2 openSUSE-SU-2015:2244-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4807, CVE-2015-4815, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4913

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2244-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00048.html

SuSE Linux 13.2
x86_64
libmysqld18-debuginfo-10.0.22-2.18.1
mariadb-debuginfo-10.0.22-2.18.1
mariadb-debugsource-10.0.22-2.18.1
mariadb-tools-debuginfo-10.0.22-2.18.1
libmysqlclient_r18-32bit-10.0.22-2.18.1
libmysqlclient18-debuginfo-32bit-10.0.22-2.18.1
mariadb-bench-10.0.22-2.18.1
libmysqlclient_r18-10.0.22-2.18.1
mariadb-errormessages-10.0.22-2.18.1
mariadb-test-10.0.22-2.18.1
libmysqlclient18-10.0.22-2.18.1
mariadb-test-debuginfo-10.0.22-2.18.1

mariadb-tools-10.0.22-2.18.1
libmysqlclient18-debuginfo-10.0.22-2.18.1
libmysqlclient-devel-10.0.22-2.18.1
mariadb-client-10.0.22-2.18.1
libmysqld-devel-10.0.22-2.18.1
mariadb-10.0.22-2.18.1
mariadb-client-debuginfo-10.0.22-2.18.1
libmysqlclient18-32bit-10.0.22-2.18.1
mariadb-bench-debuginfo-10.0.22-2.18.1
libmysqld18-10.0.22-2.18.1

i586
libmysqld18-debuginfo-10.0.22-2.18.1
mariadb-debuginfo-10.0.22-2.18.1
mariadb-debugsource-10.0.22-2.18.1
mariadb-tools-debuginfo-10.0.22-2.18.1
mariadb-bench-10.0.22-2.18.1
libmysqlclient_r18-10.0.22-2.18.1
mariadb-errormessages-10.0.22-2.18.1
mariadb-test-10.0.22-2.18.1
libmysqlclient18-10.0.22-2.18.1
mariadb-test-debuginfo-10.0.22-2.18.1
mariadb-tools-10.0.22-2.18.1
libmysqlclient18-debuginfo-10.0.22-2.18.1
libmysqlclient-devel-10.0.22-2.18.1
mariadb-client-10.0.22-2.18.1
libmysqld-devel-10.0.22-2.18.1
mariadb-10.0.22-2.18.1
mariadb-client-debuginfo-10.0.22-2.18.1
mariadb-bench-debuginfo-10.0.22-2.18.1
libmysqld18-10.0.22-2.18.1

170592 - Amazon Linux AMI ALAS-2015-626 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8169

Description

The scan detected that the host is missing the following update:
ALAS-2015-626

Observation

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

https://alas.aws.amazon.com/ALAS-2015-626.html

Amazon Linux AMI
x86_64
autofs-debuginfo-5.0.7-54.22.amzn1
autofs-5.0.7-54.22.amzn1

i686
autofs-debuginfo-5.0.7-54.22.amzn1
autofs-5.0.7-54.22.amzn1

174727 - Scientific Linux Security ERRATA Moderate: nss on SL5.x i386/x86_64 (1508-21735)

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

Risk Level: Medium

CVE: CVE-2015-2721, CVE-2015-2730

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nss on SL5.x i386/x86_64 (1508-21735)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=21735

SL5
x86_64
nss-debuginfo-3.19.1-1.el5_11
nss-tools-3.19.1-1.el5_11
nss-3.19.1-1.el5_11
nss-devel-3.19.1-1.el5_11
nss-pkcs11-devel-3.19.1-1.el5_11

i386
nss-debuginfo-3.19.1-1.el5_11
nss-tools-3.19.1-1.el5_11
nss-3.19.1-1.el5_11
nss-devel-3.19.1-1.el5_11
nss-pkcs11-devel-3.19.1-1.el5_11

174732 - Scientific Linux Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1508-3154)

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

Risk Level: Medium

CVE: CVE-2014-9297, CVE-2014-9298, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1508-3154)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=3154

SL6
i386
ntpdate-4.2.6p5-5.el6
ntp-debuginfo-4.2.6p5-5.el6
ntp-perl-4.2.6p5-5.el6
ntp-4.2.6p5-5.el6

noarch
ntp-doc-4.2.6p5-5.el6

x86_64
ntpdate-4.2.6p5-5.el6
ntp-debuginfo-4.2.6p5-5.el6
ntp-perl-4.2.6p5-5.el6
ntp-4.2.6p5-5.el6

174758 - Scientific Linux Security ERRATA Low: wpa_supplicant on SL6.x i386/x86_64 (1508-1067)

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

Risk Level: Medium

CVE: CVE-2015-4142

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: wpa_supplicant on SL6.x i386/x86_64 (1508-1067)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=1067

SL6
x86_64
wpa_supplicant-0.7.3-6.el6
wpa_supplicant-debuginfo-0.7.3-6.el6

i386
wpa_supplicant-0.7.3-6.el6
wpa_supplicant-debuginfo-0.7.3-6.el6

174759 - Scientific Linux Security ERRATA Moderate: pki-core on SL6.x i386/x86_64 (1508-5148)

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

Risk Level: Medium

CVE: CVE-2012-2662

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: pki-core on SL6.x i386/x86_64 (1508-5148)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=5148

SL6
i386
pki-native-tools-9.0.3-43.el6
pki-core-debuginfo-9.0.3-43.el6
pki-symkey-9.0.3-43.el6

noarch
pki-util-9.0.3-43.el6
pki-java-tools-javadoc-9.0.3-43.el6

pki-java-tools-9.0.3-43.el6
pki-common-9.0.3-43.el6
pki-selinux-9.0.3-43.el6
pki-ca-9.0.3-43.el6
pki-common-javadoc-9.0.3-43.el6
pki-setup-9.0.3-43.el6
pki-silent-9.0.3-43.el6
pki-util-javadoc-9.0.3-43.el6

x86_64
pki-native-tools-9.0.3-43.el6
pki-core-debuginfo-9.0.3-43.el6
pki-symkey-9.0.3-43.el6

174762 - Scientific Linux Security ERRATA Important: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-9408)

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

Risk Level: Medium

CVE: CVE-2015-4495

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1508-9408)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=9408

SL5
x86_64
firefox-38.1.1-1.el5_11
firefox-debuginfo-38.1.1-1.el5_11

i386
firefox-38.1.1-1.el5_11
firefox-debuginfo-38.1.1-1.el5_11

SL7
x86_64
firefox-38.1.1-1.el7_1
firefox-debuginfo-38.1.1-1.el7_1

SL6
x86_64
firefox-debuginfo-38.1.1-1.el6_7
firefox-38.1.1-1.el6_7

i386
firefox-debuginfo-38.1.1-1.el6_7
firefox-38.1.1-1.el6_7

174768 - Scientific Linux Security ERRATA Moderate: hivex on SL6.x x86_64 (1508-6188)

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

Risk Level: Medium

CVE: CVE-2014-9273

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: hivex on SL6.x x86_64 (1508-6188)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=6188

SL6
x86_64
hivex-debuginfo-1.3.3-4.3.el6
perl-hivex-1.3.3-4.3.el6
ocaml-hivex-1.3.3-4.3.el6
hivex-1.3.3-4.3.el6
ocaml-hivex-devel-1.3.3-4.3.el6
hivex-devel-1.3.3-4.3.el6
python-hivex-1.3.3-4.3.el6

174770 - Scientific Linux Security ERRATA Moderate: ipa on SL6.x i386/x86_64 (1508-2807)

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

Risk Level: Medium

CVE: CVE-2010-5312, CVE-2012-6662

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ipa on SL6.x i386/x86_64 (1508-2807)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=2807

SL6
x86_64
ipa-server-selinux-3.0.0-47.el6
ipa-client-3.0.0-47.el6
ipa-server-trust-ad-3.0.0-47.el6
ipa-python-3.0.0-47.el6
ipa-admintools-3.0.0-47.el6
ipa-server-3.0.0-47.el6
ipa-debuginfo-3.0.0-47.el6

i386
ipa-server-selinux-3.0.0-47.el6
ipa-client-3.0.0-47.el6
ipa-server-trust-ad-3.0.0-47.el6
ipa-python-3.0.0-47.el6
ipa-admintools-3.0.0-47.el6
ipa-server-3.0.0-47.el6
ipa-debuginfo-3.0.0-47.el6

174779 - Scientific Linux Security ERRATA Moderate: openssl on SL6.x, SL7.x i386/x86_64 (1506-2853)

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

Risk Level: Medium

CVE: CVE-2015-4000

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssl on SL6.x, SL7.x i386/x86_64 (1506-2853)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=2853

SL7
x86_64
openssl-devel-1.0.1e-42.el7_1.6
openssl-libs-1.0.1e-42.el7_1.6
openssl-1.0.1e-42.el7_1.6
openssl-debuginfo-1.0.1e-42.el7_1.6
openssl-static-1.0.1e-42.el7_1.6
openssl-perl-1.0.1e-42.el7_1.6

SL6
x86_64
openssl-static-1.0.1e-30.el6_6.9
openssl-perl-1.0.1e-30.el6_6.9
openssl-debuginfo-1.0.1e-30.el6_6.9
openssl-devel-1.0.1e-30.el6_6.9
openssl-1.0.1e-30.el6_6.9

i386
openssl-static-1.0.1e-30.el6_6.9
openssl-perl-1.0.1e-30.el6_6.9
openssl-debuginfo-1.0.1e-30.el6_6.9
openssl-devel-1.0.1e-30.el6_6.9
openssl-1.0.1e-30.el6_6.9

174781 - Scientific Linux Security ERRATA Moderate: libreswan on SL7.x x86_64 (1511-1678)

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

Risk Level: Medium

CVE: CVE-2015-3240

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: libreswan on SL7.x x86_64 (1511-1678)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1511&L=scientific-linux-errata&F=&S=&P=1678

SL7
x86_64
libreswan-3.15-5.el7_1
libreswan-debuginfo-3.15-5.el7_1

174788 - Scientific Linux Security ERRATA Moderate: nss-softokn on SL6.x, SL7.x i386/x86_64 (1509-5841)

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

Risk Level: Medium

CVE: CVE-2015-2730

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nss-softokn on SL6.x, SL7.x i386/x86_64 (1509-5841)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1509&L=scientific-linux-errata&F=&S=&P=5841

SL7
x86_64
nss-softokn-devel-3.16.2.3-13.el7_1
nss-softokn-debuginfo-3.16.2.3-13.el7_1
nss-softokn-freebl-3.16.2.3-13.el7_1
nss-softokn-3.16.2.3-13.el7_1
nss-softokn-freebl-devel-3.16.2.3-13.el7_1

SL6
x86_64
nss-softokn-debuginfo-3.14.3-23.el6_7
nss-softokn-freebl-devel-3.14.3-23.el6_7
nss-softokn-devel-3.14.3-23.el6_7
nss-softokn-freebl-3.14.3-23.el6_7
nss-softokn-3.14.3-23.el6_7

i386
nss-softokn-debuginfo-3.14.3-23.el6_7
nss-softokn-freebl-devel-3.14.3-23.el6_7
nss-softokn-devel-3.14.3-23.el6_7
nss-softokn-freebl-3.14.3-23.el6_7
nss-softokn-3.14.3-23.el6_7

174799 - Scientific Linux Security ERRATA Moderate: postgresql on SL6.x, SL7.x i386/x86_64 (1506-15210)

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

Risk Level: Medium

CVE: CVE-2015-3165, CVE-2015-3166, CVE-2015-3167

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL6.x, SL7.x i386/x86_64 (1506-15210)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=15210

SL7
x86_64
postgresql-9.2.13-1.el7_1
postgresql-test-9.2.13-1.el7_1
postgresql-upgrade-9.2.13-1.el7_1
postgresql-plpython-9.2.13-1.el7_1
postgresql-server-9.2.13-1.el7_1
postgresql-docs-9.2.13-1.el7_1
postgresql-contrib-9.2.13-1.el7_1
postgresql-libs-9.2.13-1.el7_1
postgresql-debuginfo-9.2.13-1.el7_1
postgresql-pltcl-9.2.13-1.el7_1
postgresql-devel-9.2.13-1.el7_1
postgresql-plperl-9.2.13-1.el7_1

SL6
x86_64
postgresql-test-8.4.20-3.el6_6
postgresql-libs-8.4.20-3.el6_6
postgresql-docs-8.4.20-3.el6_6
postgresql-contrib-8.4.20-3.el6_6
postgresql-plperl-8.4.20-3.el6_6
postgresql-debuginfo-8.4.20-3.el6_6
postgresql-pltcl-8.4.20-3.el6_6
postgresql-devel-8.4.20-3.el6_6
postgresql-plpython-8.4.20-3.el6_6
postgresql-8.4.20-3.el6_6
postgresql-server-8.4.20-3.el6_6

i386
postgresql-test-8.4.20-3.el6_6
postgresql-libs-8.4.20-3.el6_6
postgresql-docs-8.4.20-3.el6_6
postgresql-contrib-8.4.20-3.el6_6
postgresql-plperl-8.4.20-3.el6_6
postgresql-debuginfo-8.4.20-3.el6_6
postgresql-pltcl-8.4.20-3.el6_6
postgresql-devel-8.4.20-3.el6_6
postgresql-plpython-8.4.20-3.el6_6
postgresql-8.4.20-3.el6_6
postgresql-server-8.4.20-3.el6_6

174808 - Scientific Linux Security ERRATA Low: grep on SL6.x i386/x86_64 (1508-3964)

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

Risk Level: Medium

CVE: CVE-2012-5667, CVE-2015-1345

Description

The scan detected that the host is missing the following update:
Security ERRATA Low: grep on SL6.x i386/x86_64 (1508-3964)

Observation

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

For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=3964

SL6
x86_64
grep-debuginfo-2.20-3.el6
grep-2.20-3.el6

i386
grep-debuginfo-2.20-3.el6
grep-2.20-3.el6

174815 - Scientific Linux Security ERRATA Moderate: autofs on SL6.x i386/x86_64 (1508-6876)

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

Risk Level: Medium

CVE: CVE-2014-8169

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: autofs on SL6.x i386/x86_64 (1508-6876)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1508&L=scientific-linux-errata&F=&S=&P=6876

SL6
x86_64
autofs-debuginfo-5.0.5-113.el6
autofs-5.0.5-113.el6

i386
autofs-debuginfo-5.0.5-113.el6
autofs-5.0.5-113.el6

174829 - Scientific Linux Security ERRATA Moderate: nss on SL6.x, SL7.x i386/x86_64 (1506-14561)

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

Risk Level: Medium

CVE: CVE-2015-4000

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: nss on SL6.x, SL7.x i386/x86_64 (1506-14561)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1506&L=scientific-linux-errata&F=&S=&P=14561

SL7
x86_64

nss-sysinit-3.19.1-3.el7_1
nss-util-3.19.1-1.el7_1
nss-util-devel-3.19.1-1.el7_1
nss-3.19.1-3.el7_1
nss-util-debuginfo-3.19.1-1.el7_1
nss-debuginfo-3.19.1-3.el7_1
nss-pkcs11-devel-3.19.1-3.el7_1
nss-tools-3.19.1-3.el7_1
nss-devel-3.19.1-3.el7_1

SL6
x86_64
nss-util-3.19.1-1.el6_6
nss-util-debuginfo-3.19.1-1.el6_6
nss-debuginfo-3.19.1-3.el6_6
nss-util-devel-3.19.1-1.el6_6
nss-devel-3.19.1-3.el6_6
nss-sysinit-3.19.1-3.el6_6
nss-pkcs11-devel-3.19.1-3.el6_6
nss-3.19.1-3.el6_6
nss-tools-3.19.1-3.el6_6

i386
nss-util-3.19.1-1.el6_6
nss-util-debuginfo-3.19.1-1.el6_6
nss-debuginfo-3.19.1-3.el6_6
nss-util-devel-3.19.1-1.el6_6
nss-devel-3.19.1-3.el6_6
nss-sysinit-3.19.1-3.el6_6
nss-pkcs11-devel-3.19.1-3.el6_6
nss-3.19.1-3.el6_6
nss-tools-3.19.1-3.el6_6

178076 - Gentoo Linux GLSA-201507-22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1572

Description

The scan detected that the host is missing the following update:
GLSA-201507-22

Observation

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

https://security.gentoo.org/glsa/201507-22

Affected packages:
sys-fs/e2fsprogs < 1.42.13

178090 - Gentoo Linux GLSA-201507-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8161, CVE-2015-0241, CVE-2015-0242, CVE-2015-0243, CVE-2015-0244, CVE-2015-3165, CVE-2015-3166, CVE-

2015-3167

Description

The scan detected that the host is missing the following update:
GLSA-201507-20

Observation

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

https://security.gentoo.org/glsa/201507-20

Affected packages:
dev-db/postgresql < 9.4.3

178098 - Gentoo Linux GLSA-201509-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1798, CVE-2015-1799, CVE-2015-5146

Description

The scan detected that the host is missing the following update:
GLSA-201509-01

Observation

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

https://security.gentoo.org/glsa/201509-01

Affected packages:
net-misc/ntp < 4.2.8_p3

178110 - Gentoo Linux GLSA-201503-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9273

Description

The scan detected that the host is missing the following update:
GLSA-201503-07

Observation

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

https://security.gentoo.org/glsa/201503-07

Affected packages:
app-misc/hivex < 1.3.11

181708 - FreeBSD redmine Multiple Vulnerabilities (0e0385d1-9ed5-11e5-8f5c-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2012-0327

Description

The scan detected that the host is missing the following update:
redmine -- multiple vulnerabilities (0e0385d1-9ed5-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/0e0385d1-9ed5-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 1.3.2

190084 - Fedora Linux 22 FEDORA-2015-c4ed00a68f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7515, CVE-2015-7833, CVE-2015-8374

Description

The scan detected that the host is missing the following update:
FEDORA-2015-c4ed00a68f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173888.html

Fedora Core 22

kernel-4.2.7-200.fc22

190096 - Fedora Linux 23 FEDORA-2015-ac9a19888e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7515, CVE-2015-7833, CVE-2015-8374

Description

The scan detected that the host is missing the following update:
FEDORA-2015-ac9a19888e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173908.html

Fedora Core 23

kernel-4.2.7-300.fc23

33316 - Oracle Solaris 146289-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
146289-03

Observation

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

https://getupdates.oracle.com/readme/146289-03

SunOS 5.10(x86): dcfs patch

SOLARIS_10_x86

SUNWckr:11.10.0,REV=2005.01.21.16.34

33317 - Oracle Solaris 146288-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
146288-03

Observation

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

https://getupdates.oracle.com/readme/146288-03

SunOS 5.10: dcfs patch

SOLARIS_10

SUNWckr:11.10.0,REV=2005.01.21.15.53

88725 - Slackware Linux 14.1 SSA:2015-349-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2015-349-03

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.356015

Slackware 14.1
x86_64
mozilla-firefox-38.5.0esr-x86_64-1

130332 - Debian Linux 8.0 DSA-3419-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8560

Description

The scan detected that the host is missing the following update:
DSA-3419-1

Observation

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

http://www.debian.org/security/2015/dsa-3419

Debian 8.0
all
cups-filters_1.0.61-5+deb8u3

130334 - Debian Linux 7.0, 8.0 DSA-3420-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
DSA-3420-1

Observation

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

http://www.debian.org/security/2015/dsa-3420

Debian 8.0
all
bind9_1:9.9.5.dfsg-9+deb8u4

Debian 7.0

all
bind9_1:9.8.4.dfsg.P1-6+nmu2+deb7u8

130337 - Debian Linux 7.0, 8.0 DSA-3416-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8476

Description

The scan detected that the host is missing the following update:
DSA-3416-1

Observation

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

http://www.debian.org/security/2015/dsa-3416

Debian 8.0
all
libphp-phpmailer_5.2.9+dfsg-2+deb8u1

Debian 7.0
all
libphp-phpmailer_5.1-1.1

144091 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2256-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8367

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:2256-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-12/msg00056.html

SuSE Linux 13.1
x86_64
libraw9-debuginfo-0.15.4-2.6.1
libraw-devel-0.15.4-2.6.1
libraw-devel-static-0.15.4-2.6.1
libraw-tools-0.15.4-2.6.1
libraw-tools-debuginfo-0.15.4-2.6.1
libraw-debugsource-0.15.4-2.6.1
libraw9-0.15.4-2.6.1

i586
libraw9-debuginfo-0.15.4-2.6.1
libraw-devel-0.15.4-2.6.1

libraw-devel-static-0.15.4-2.6.1
libraw-tools-0.15.4-2.6.1
libraw-tools-debuginfo-0.15.4-2.6.1
libraw-debugsource-0.15.4-2.6.1
libraw9-0.15.4-2.6.1

SuSE Linux 13.2
x86_64
libraw-devel-static-0.16.0-2.6.1
libraw10-0.16.0-2.6.1
libraw-devel-0.16.0-2.6.1
libraw-debugsource-0.16.0-2.6.1
libraw10-debuginfo-0.16.0-2.6.1
libraw-tools-debuginfo-0.16.0-2.6.1
libraw-tools-0.16.0-2.6.1

i586
libraw-devel-static-0.16.0-2.6.1
libraw10-0.16.0-2.6.1
libraw-devel-0.16.0-2.6.1
libraw-debugsource-0.16.0-2.6.1
libraw10-debuginfo-0.16.0-2.6.1
libraw-tools-debuginfo-0.16.0-2.6.1
libraw-tools-0.16.0-2.6.1

170593 - Amazon Linux AMI ALAS-2015-627 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8326

Description

The scan detected that the host is missing the following update:
ALAS-2015-627

Observation

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

https://alas.aws.amazon.com/ALAS-2015-627.html

Amazon Linux AMI
noarch
perl-IPTables-Parse-1.5-2.3.amzn1

178089 - Gentoo Linux GLSA-201509-05 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2924

Description

The scan detected that the host is missing the following update:
GLSA-201509-05

Observation

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

https://security.gentoo.org/glsa/201509-05

Affected packages:
net-misc/networkmanager < 1.0.2

181702 - FreeBSD redmine CSRF Protection Bypass (ae377aeb-9ed4-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
redmine -- CSRF protection bypass (ae377aeb-9ed4-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/ae377aeb-9ed4-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 1.3.0

181703 - FreeBSD jenkins Multiple Vulnerabilities (23af0425-9eac-11e5-b937-00e0814cab4e)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
jenkins -- multiple vulnerabilities (23af0425-9eac-11e5-b937-00e0814cab4e)

Observation

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

http://www.vuxml.org/freebsd/23af0425-9eac-11e5-b937-00e0814cab4e.html

Affected packages:
jenkins <= 1.641
jenkins-lts <= 1.625.3

181706 - FreeBSD redmine XSS Vulnerability (66ba5931-9ed5-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
redmine -- XSS vulnerability (66ba5931-9ed5-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/66ba5931-9ed5-11e5-8f5c-002590263bf5.html

Affected packages:
2.1.0 <= redmine < 2.1.2

181707 - FreeBSD redmine Open Redirect Vulnerability (3ec2e0bc-9ed7-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8474

Description

The scan detected that the host is missing the following update:
redmine -- open redirect vulnerability (3ec2e0bc-9ed7-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/3ec2e0bc-9ed7-11e5-8f5c-002590263bf5.html

Affected packages:
2.5.1 <= redmine < 2.6.7
3.0.0 <= redmine < 3.0.5
redmine == 3.1.0

181709 - FreeBSD redmine Multiple Vulnerabilities (be63533c-9ed7-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8346, CVE-2015-8473

Description

The scan detected that the host is missing the following update:
redmine -- multiple vulnerabilities (be63533c-9ed7-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/be63533c-9ed7-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 2.6.8
3.0.0 <= redmine < 3.0.6
3.1.0 <= redmine < 3.1.2

181711 - FreeBSD subversion Multiple Vulnerabilities (daadef86-a366-11e5-8b40-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2015-5259, CVE-2015-5343

Description

The scan detected that the host is missing the following update:
subversion -- multiple vulnerabilities (daadef86-a366-11e5-8b40-20cf30e32f6d)

Observation

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

http://www.vuxml.org/freebsd/daadef86-a366-11e5-8b40-20cf30e32f6d.html

Affected packages:
1.7.0 <= subversion17 < 1.7.22_1
1.8.0 <= subversion18 < 1.8.15
1.9.0 <= subversion < 1.9.3
1.7.0 <= mod_dav_svn < 1.7.22_1
1.8.0 <= mod_dav_svn < 1.8.15
1.9.0 <= mod_dav_svn < 1.9.3

181712 - FreeBSD redmine Information Leak Vulnerability (21bc4d71-9ed8-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8537

Description

The scan detected that the host is missing the following update:
redmine -- information leak vulnerability (21bc4d71-9ed8-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/21bc4d71-9ed8-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 2.6.9
3.0.0 <= redmine < 3.0.7
3.1.0 <= redmine < 3.1.3

181714 - FreeBSD redmine Potential XSS Vulnerability (939a7086-9ed6-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8477

Description

The scan detected that the host is missing the following update:
redmine -- potential XSS vulnerability (939a7086-9ed6-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/939a7086-9ed6-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 2.6.2

181715 - FreeBSD redmine Information Leak Vulnerability (49def4b7-9ed6-11e5-8f5c-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
redmine -- information leak vulnerability (49def4b7-9ed6-11e5-8f5c-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/49def4b7-9ed6-11e5-8f5c-002590263bf5.html

Affected packages:
redmine < 2.4.6
2.5.0 <= redmine < 2.5.2

185079 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2836-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
USN-2836-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003218.html

Ubuntu 12.04

grub2-common_1.99-21ubuntu3.19

Ubuntu 15.04

grub2-common_2.02~beta2-22ubuntu1.4

Ubuntu 15.10

grub2-common_2.02~beta2-29ubuntu0.2

Ubuntu 14.04

grub2-common_2.02~beta2-9ubuntu1.6

185080 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2837-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8000

Description

The scan detected that the host is missing the following update:
USN-2837-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003219.html

Ubuntu 12.04

bind9_9.8.1.dfsg.P1-4ubuntu0.14

Ubuntu 15.04

bind9_9.9.5.dfsg-9ubuntu0.4

Ubuntu 15.10

bind9_9.9.5.dfsg-11ubuntu1.1

Ubuntu 14.04

bind9_9.9.5.dfsg-3ubuntu0.6

185081 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2835-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7545

Description

The scan detected that the host is missing the following update:
USN-2835-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003217.html

Ubuntu 12.04

git_1.7.9.5-1ubuntu0.2

Ubuntu 15.04

git_2.1.4-2.1ubuntu0.1

Ubuntu 15.10

git_2.5.0-1ubuntu0.1

Ubuntu 14.04

git_1.9.1-1ubuntu0.2

185084 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2834-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317

Description

The scan detected that the host is missing the following update:
USN-2834-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003216.html

Ubuntu 12.04

libxml2_2.7.8.dfsg-5.1ubuntu4.13

Ubuntu 15.04

libxml2_2.9.2+dfsg1-3ubuntu0.2

Ubuntu 15.10

libxml2_2.9.2+zdfsg1-4ubuntu0.2

Ubuntu 14.04

libxml2_2.9.1+dfsg1-3ubuntu4.6

190085 - Fedora Linux 23 FEDORA-2015-df0f324367 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-2015-df0f324367

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173549.html

Fedora Core 23

knot-2.0.2-1.fc23

190086 - Fedora Linux 22 FEDORA-2015-c7b1be8823 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-2015-c7b1be8823

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173894.html

Fedora Core 22

seamonkey-2.39-1.fc22

190087 - Fedora Linux 23 FEDORA-2015-b2e8518b8e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8504

Description

The scan detected that the host is missing the following update:
FEDORA-2015-b2e8518b8e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173749.html

Fedora Core 23

qemu-2.4.1-3.fc23

190088 - Fedora Linux 22 FEDORA-2015-2ebdd4ad8f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5264, CVE-2015-5265, CVE-2015-5266, CVE-2015-5267, CVE-2015-5268, CVE-2015-5269, CVE-2015-5272, CVE-2015-5331, CVE-2015-5332, CVE-2015-5335, CVE-2015-5336, CVE-2015-5337, CVE-2015-5338, CVE-2015-5339, CVE-2015-5340, CVE-2015-5341, CVE-2015-5342

Description

The scan detected that the host is missing the following update:
FEDORA-2015-2ebdd4ad8f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173666.html

Fedora Core 22

moodle-2.8.9-1.fc22

190089 - Fedora Linux 23 FEDORA-2015-cebe5133e7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8370

Description

The scan detected that the host is missing the following update:
FEDORA-2015-cebe5133e7

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173703.html

Fedora Core 23

grub2-2.02-0.25.fc23

190090 - Fedora Linux 22 FEDORA-2015-97055df8a0 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-2015-97055df8a0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173688.html

Fedora Core 22

proftpd-1.3.5a-5.fc22

190091 - Fedora Linux 22 FEDORA-2015-fff2073f50 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-2015-fff2073f50

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173812.html

Fedora Core 22

wget-1.16.3-2.fc22

190092 - Fedora Linux 22 FEDORA-2015-a288773b9a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8366, CVE-2015-8367

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a288773b9a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173691.html

Fedora Core 22

LibRaw-0.16.2-3.fc22

190093 - Fedora Linux 23 FEDORA-2015-7a89e8db70 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-2015-7a89e8db70

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173656.html

Fedora Core 23

proftpd-1.3.5a-5.fc23

190094 - Fedora Linux 23 FEDORA-2015-98fc0d20ad Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5264, CVE-2015-5265, CVE-2015-5266, CVE-2015-5267, CVE-2015-5268, CVE-2015-5269, CVE-2015-5272, CVE-2015-5331, CVE-2015-5332, CVE-2015-5335, CVE-2015-5336, CVE-2015-5337, CVE-2015-5338, CVE-2015-5339, CVE-2015-5340, CVE-2015-5341, CVE-2015-5342

Description

The scan detected that the host is missing the following update:
FEDORA-2015-98fc0d20ad

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173618.html

Fedora Core 23

moodle-2.9.3-1.fc23

190095 - Fedora Linux 22 FEDORA-2015-b5a8f09e32 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-2015-b5a8f09e32

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173564.html

Fedora Core 22

knot-1.6.6-1.fc22

190097 - Fedora Linux 22 FEDORA-2015-6565f29415 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-2015-6565f29415

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173807.html

Fedora Core 22

pax-utils-1.1.4-1.fc22

190098 - Fedora Linux 23 FEDORA-2015-28e56e52e7 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-2015-28e56e52e7

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173925.html

Fedora Core 23

seamonkey-2.39-1.fc23

190100 - Fedora Linux 23 FEDORA-2015-73cdd43bc0 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-2015-73cdd43bc0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173515.html

Fedora Core 23

pax-utils-1.1.4-1.fc23

170599 - Amazon Linux AMI ALAS-2015-629 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5667

Description

The scan detected that the host is missing the following update:
ALAS-2015-629

Observation

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

https://alas.aws.amazon.com/ALAS-2015-629.html

Amazon Linux AMI
noarch
perl-HTML-Scrubber-0.15-1.5.amzn1

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.

19383 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.73

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

Risk Level: High

CVE: CVE-2015-6764, CVE-2015-6765, CVE-2015-6766, CVE-2015-6767, CVE-2015-6768, CVE-2015-6769, CVE-2015-6770, CVE-2015-6771, CVE-2015-6772, CVE-2015-6773, CVE-2015-6774, CVE-2015-6775, CVE-2015-6776, CVE-2015-6777, CVE-2015-6778, CVE-2015-6779, CVE-2015-6780, CVE-2015-6781, CVE-2015-6782, CVE-2015-6783, CVE-2015-6784, CVE-2015-6785, CVE-2015-6786, CVE-2015-6787, CVE-2015-8478

Update Details

CVE is updated

19387 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.73

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6764, CVE-2015-6765, CVE-2015-6766, CVE-2015-6767, CVE-2015-6768, CVE-2015-6769, CVE-2015-6770, CVE-2015-6771, CVE-2015-6772, CVE-2015-6773, CVE-2015-6774, CVE-2015-6775, CVE-2015-6776, CVE-2015-6777, CVE-2015-6778, CVE-2015-6779, CVE-2015-6780, CVE-2015-6781, CVE-2015-6782, CVE-2015-6783, CVE-2015-6784, CVE-2015-6785, CVE-2015-6786, CVE-2015-6787, CVE-2015-8478

Update Details

CVE is updated

19426 - (APSB15-32) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8051, CVE-2015-8052, CVE-2015-8053, CVE-2015-8054, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8456, CVE-2015-8457

Update Details

CVE is updated

19427 - (APSB15-32) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8051, CVE-2015-8052, CVE-2015-8053, CVE-2015-8054, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8456, CVE-2015-8457

Update Details

CVE is updated

144001 - SuSE Linux 11.4 openSUSE-SU-2015:1781-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3107, CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5567, CVE-2015-5568, CVE-2015-5569, CVE-2015-5570, CVE-2015-5571, CVE-2015-5572, CVE-2015-5573, CVE-2015-5574, CVE-2015-5575, CVE-2015-5576, CVE-2015-5577, CVE-2015-5578, CVE-2015-5579, CVE-2015-5580, CVE-2015-5581, CVE-2015-5582, CVE-2015-5584, CVE-2015-5587, CVE-2015-5588, CVE-2015-6676, CVE-2015-6677, CVE-2015-6678, CVE-2015-6679, CVE-2015-6682, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628, CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE-2015-7634, CVE-2015-7643, CVE-2015-7644, CVE-2015-7645

Update Details

CVE is updated

18985 - (MS15-098) Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2513, CVE-2015-2514, CVE-2015-2516, CVE-2015-2519, CVE-2015-2530

Update Details

Documentation is updated

144047 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2000-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9756, CVE-2015-7805

Update Details

CVE is updated

144050 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1995-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9756, CVE-2015-7805

Update Details

CVE is updated

19014 - (SOL17181) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5722

Update Details

Recommendation is updated Documentation is updated

18705 - (SOL16870) F5 BIG-IP logrotate Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2011-1154

Update Details

Documentation is updated

18716 - (SOL16821) F5 BIG-IP Apache Axis Spoofing Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-3596

Update Details

Documentation is updated

91942 - Oracle Enterprise Linux ELSA-2015-2231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405, CVE-2015-5300, CVE-2015-7704

Update Details

CVE is updated

141017 - Red Hat Enterprise Linux RHSA-2015-2231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2014-9751, CVE-2015-1798, CVE-2015-1799, CVE-2015-3405

Update Details

CVE is updated

18714 - (SOL16826) F5 BIG-IP PHP Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-4024

Update Details

Documentation is updated

88715 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-302-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, 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

Update Details

CVE is updated

18707 - (SOL16859) F5 BIG-IP SUSE coreutils Multiple Denial Of Service Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-0221, CVE-2013-0222, CVE-2013-0223

Update Details

Documentation is updated

130297 - Debian Linux 7.0, 8.0 DSA-3380-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7803, CVE-2015-7804

Update Details
Risk is updated

170578 - Amazon Linux AMI ALAS-2015-601 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-6834, CVE-2015-6835, CVE-2015-7803, CVE-2015-7804

Update Details
Risk is updated

170579 - Amazon Linux AMI ALAS-2015-602 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-6834, CVE-2015-6835, CVE-2015-7803, CVE-2015-7804

Update Details
Risk is updated

181406 - FreeBSD ufraw Integer Overflow Condition (57325ecf-facc-11e4-968f-b888e347c638)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-3885

Update Details
FASLScript is updated

181626 - FreeBSD php Multiple Vulnerabilities (c1da8b75-6aef-11e5-9909-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7803, CVE-2015-7804

Update Details
Risk is updated

185031 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2786-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7803, CVE-2015-7804

Update Details

Risk is updated

170569 - Amazon Linux AMI ALAS-2015-593 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3405, CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7703

Update Details

CVE is updated

181638 - FreeBSD Git Execute Arbitrary Code (7f645ee5-7681-11e5-8519-005056ac623e)

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

Risk Level: Low

CVE: CVE-2015-7545

Update Details

CVE is updated

185028 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2783-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, 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-2015-7850, CVE-2015-7852, CVE-2015-7853, CVE-2015-7855, CVE-2015-7871

Update Details

CVE is updated

189755 - Fedora Linux 23 FEDORA-2015-14213 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7703

Update Details

CVE is updated

189817 - Fedora Linux 22 FEDORA-2015-14212 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7703

Update Details

CVE is updated

189942 - Fedora Linux 21 FEDORA-2015-77bfbc1bcd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7852, CVE-2015-7871

Update Details

CVE is updated

18699 - (SOL16869) F5 BIG-IP logrotate Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2011-1098

Update Details

Documentation is updated

18704 - (SOL16871) F5 BIG-IP logrotate Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2011-1155

Update Details

Documentation is updated

14416 - Oracle Database Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14432 - Adobe Macromedia Flash Player Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14506 - Adobe Acrobat Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14534 - Microsoft Internet Information Services (IIS) Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14541 - HP Systems Insight Manager Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

14542 - Mozilla Firefox Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

15211 - VMware Fusion Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70014 - netbios-helpers.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70116 - scada.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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