2014-NOV-06
FSL version 7.5.644

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

17298 - (HT6537) Apple iTunes Multiple Vulnerabilities Prior To 12.0.1

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

Risk Level: High

CVE: CVE-2013-2871, CVE-2013-2875, CVE-2013-2909, CVE-2013-2926, CVE-2013-2927, CVE-2013-2928, CVE-2013-5195, CVE-2013-5196, CVE-2013-5197, CVE-2013-5198, CVE-2013-5199, CVE-2013-5225, CVE-2013-5228, CVE-2013-6625, CVE-2013-6635, CVE-2013-6663, CVE-2014-1268, CVE-2014-1269, CVE-2014-1270, CVE-2014-1289, CVE-2014-1290, CVE-2014-1291, CVE-2014-1292, CVE-2014-1293, CVE-2014-1294, CVE-2014-1298, CVE-2014-1299, CVE-2014-1300, CVE-2014-1301, CVE-2014-1302, CVE-2014-1303, CVE-2014-1304, CVE-2014-1305, CVE-2014-1307, CVE-2014-1308, CVE-2014-1309, CVE-2014-1310, CVE-2014-1311, CVE-2014-1312, CVE-2014-1313, CVE-2014-1323, CVE-2014-1324, CVE-2014-1325, CVE-2014-1326, CVE-2014-1327, CVE-2014-1329, CVE-2014-1330, CVE-2014-1331, CVE-2014-1333, CVE-2014-1334, CVE-2014-1335, CVE-2014-1336, CVE-2014-1337, CVE-2014-1338, CVE-2014-1339, CVE-2014-1340, CVE-2014-1341, CVE-2014-1342, CVE-2014-1343, CVE-2014-1344, CVE-2014-1362, CVE-2014-1363, CVE-2014-1364, CVE-2014-1365, CVE-2014-1366, CVE-2014-1367, CVE-2014-1368, CVE-2014-1382, CVE-2014-1384, CVE-2014-1385, CVE-2014-1386, CVE-2014-1387, CVE-2014-1388, CVE-2014-1389, CVE-2014-1390, CVE-2014-1713, CVE-2014-1731, CVE-2014-4410, CVE-2014-4411, CVE-2014-4412, CVE-2014-4413, CVE-2014-4414, CVE-2014-4415

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a popular software used to manage music, games, applications, etc.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service or execute remote code.

140600 - Red Hat Enterprise Linux RHSA-2014-1744 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6639, CVE-2013-6640, CVE-2013-6650, CVE-2013-6668, CVE-2014-1704, CVE-2014-5256

Description

The scan detected that the host is missing the following update:
RHSA-2014-1744

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1744.html

RHEL6WS

x86_64
v8314-v8-devel-3.14.5.10-6.el6
v8314-v8-3.14.5.10-6.el6
v8314-v8-debuginfo-3.14.5.10-6.el6

RHEL7WS
x86_64
v8314-v8-debuginfo-3.14.5.10-6.el7
v8314-v8-3.14.5.10-6.el7
v8314-v8-devel-3.14.5.10-6.el7

RHEL6S
x86_64
v8314-v8-devel-3.14.5.10-6.el6
v8314-v8-3.14.5.10-6.el6
v8314-v8-debuginfo-3.14.5.10-6.el6

RHEL7S
x86_64
v8314-v8-debuginfo-3.14.5.10-6.el7
v8314-v8-3.14.5.10-6.el7
v8314-v8-devel-3.14.5.10-6.el7

142480 - SuSE Linux 12.3 openSUSE-SU-2014:1344-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1554, 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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1344-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00001.html

SuSE Linux 12.3
i586
MozillaFirefox-33.0-1.90.1
libfreebl3-3.17.1-1.59.1
mozilla-nss-sysinit-3.17.1-1.59.1
seamonkey-debugsource-2.30-1.61.1
MozillaFirefox-branding-upstream-33.0-1.90.1
mozilla-nss-devel-3.17.1-1.59.1
MozillaFirefox-translations-common-33.0-1.90.1
mozilla-nss-certs-debuginfo-3.17.1-1.59.1
MozillaFirefox-translations-other-33.0-1.90.1
mozilla-nss-3.17.1-1.59.1
MozillaFirefox-debugsource-33.0-1.90.1
seamonkey-dom-inspector-2.30-1.61.1
seamonkey-translations-common-2.30-1.61.1
mozilla-nspr-4.10.7-1.34.1
libfreebl3-debuginfo-3.17.1-1.59.1
seamonkey-debuginfo-2.30-1.61.1

mozilla-nss-tools-3.17.1-1.59.1
MozillaFirefox-debuginfo-33.0-1.90.1
mozilla-nspr-debuginfo-4.10.7-1.34.1
mozilla-nss-tools-debuginfo-3.17.1-1.59.1
libsoftokn3-3.17.1-1.59.1
mozilla-nss-debuginfo-3.17.1-1.59.1
mozilla-nspr-devel-4.10.7-1.34.1
MozillaFirefox-buildsymbols-33.0-1.90.1
mozilla-nss-certs-3.17.1-1.59.1
seamonkey-2.30-1.61.1
libsoftokn3-debuginfo-3.17.1-1.59.1
mozilla-nss-sysinit-debuginfo-3.17.1-1.59.1
mozilla-nss-debugsource-3.17.1-1.59.1
seamonkey-translations-other-2.30-1.61.1
mozilla-nspr-debugsource-4.10.7-1.34.1
seamonkey-irc-2.30-1.61.1
MozillaFirefox-devel-33.0-1.90.1

x86_64
libfreebl3-debuginfo-32bit-3.17.1-1.59.1
mozilla-nss-sysinit-32bit-3.17.1-1.59.1
mozilla-nss-certs-32bit-3.17.1-1.59.1
mozilla-nspr-32bit-4.10.7-1.34.1
mozilla-nss-32bit-3.17.1-1.59.1
libsoftokn3-debuginfo-32bit-3.17.1-1.59.1
mozilla-nss-sysinit-debuginfo-32bit-3.17.1-1.59.1
libsoftokn3-32bit-3.17.1-1.59.1
mozilla-nss-certs-debuginfo-32bit-3.17.1-1.59.1
libfreebl3-32bit-3.17.1-1.59.1
mozilla-nss-debuginfo-32bit-3.17.1-1.59.1
mozilla-nspr-debuginfo-32bit-4.10.7-1.34.1

142481 - SuSE Linux 13.1 openSUSE-SU-2014:1345-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1554, 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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1345-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00002.html

SuSE Linux 13.1
i586
MozillaFirefox-translations-common-33.0-46.2
MozillaFirefox-debugsource-33.0-46.2
MozillaFirefox-branding-upstream-33.0-46.2
libfreebl3-3.17.1-43.1
seamonkey-translations-other-2.30-36.2
seamonkey-debuginfo-2.30-36.2
MozillaFirefox-devel-33.0-46.2

libsoftokn3-3.17.1-43.1
mozilla-nss-sysinit-debuginfo-3.17.1-43.1
MozillaFirefox-debuginfo-33.0-46.2
seamonkey-irc-2.30-36.2
mozilla-nss-tools-3.17.1-43.1
mozilla-nss-certs-3.17.1-43.1
mozilla-nss-sysinit-3.17.1-43.1
mozilla-nss-debuginfo-3.17.1-43.1
mozilla-nspr-debugsource-4.10.7-16.1
seamonkey-debugsource-2.30-36.2
mozilla-nss-devel-3.17.1-43.1
mozilla-nspr-devel-4.10.7-16.1
libfreebl3-debuginfo-3.17.1-43.1
seamonkey-translations-common-2.30-36.2
mozilla-nss-tools-debuginfo-3.17.1-43.1
mozilla-nss-3.17.1-43.1
mozilla-nss-certs-debuginfo-3.17.1-43.1
libsoftokn3-debuginfo-3.17.1-43.1
mozilla-nspr-4.10.7-16.1
seamonkey-dom-inspector-2.30-36.2
mozilla-nspr-debuginfo-4.10.7-16.1
mozilla-nss-debugsource-3.17.1-43.1
MozillaFirefox-33.0-46.2
MozillaFirefox-translations-other-33.0-46.2
MozillaFirefox-buildsymbols-33.0-46.2
seamonkey-2.30-36.2

x86_64
mozilla-nspr-debuginfo-32bit-4.10.7-16.1
mozilla-nss-32bit-3.17.1-43.1
mozilla-nss-certs-32bit-3.17.1-43.1
mozilla-nss-certs-debuginfo-32bit-3.17.1-43.1
mozilla-nspr-32bit-4.10.7-16.1
mozilla-nss-sysinit-debuginfo-32bit-3.17.1-43.1
libfreebl3-32bit-3.17.1-43.1
mozilla-nss-debuginfo-32bit-3.17.1-43.1
libfreebl3-debuginfo-32bit-3.17.1-43.1
libsoftokn3-32bit-3.17.1-43.1
libsoftokn3-debuginfo-32bit-3.17.1-43.1
mozilla-nss-sysinit-32bit-3.17.1-43.1

17307 - (HT6536) Apple OS X Server Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2013-3919, CVE-2013-4164, CVE-2013-4854, CVE-2013-6393, CVE-2014-0060, CVE-2014-0061, CVE-2014-0062, CVE-2014-0063, CVE-2014-0064, CVE-2014-0065, CVE-2014-0066, CVE-2014-0591, CVE-2014-3566, CVE-2014-4406, CVE-2014-4424, CVE-2014-4446, CVE-2014-4447

Description

Multiple vulnerabilities are present in some versions of Apple Mac OS X Server.

Observation

Apple Mac OS X Server provides easy to use interface to configure enterprise services for Apple devices.

Multiple vulnerabilities are present in some versions of Apple Mac OS X Server. The flaw lies in several embedded components. Successful exploitation could allow an attacker to execute arbitrary code.

58984 - Debian Linux 7.0 DSA-3062-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
DSA-3062-1

Observation

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

http://www.debian.org/security/2014/dsa-3062

Debian 7.0
all
wget_1.13.4-3+deb7u2

85817 - CentOS 6, 7 CESA-2014-1764 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
CESA-2014-1764

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-October/020721.html
http://lists.centos.org/pipermail/centos-announce/2014-October/020720.html

CentOS 7
x86_64
wget-1.14-10.el7_0.1

CentOS 6
i686
wget-1.12-5.el6_6.1

x86_64
wget-1.12-5.el6_6.1

88644 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-302-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
SSA:2014-302-01

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=2014&m=slackware-security.493450

Slackware 13.1
x86_64
wget-1.12-x86_64-2

Slackware 14.0
x86_64
wget-1.14-x86_64-2

Slackware 13.37
x86_64
wget-1.12-x86_64-2

Slackware 14.1
x86_64
wget-1.14-x86_64-3

Slackware 13.0
x86_64
wget-1.11.4-x86_64-2

91649 - Oracle Enterprise Linux ELSA-2014-1764 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
ELSA-2014-1764

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004596.html
http://oss.oracle.com/pipermail/el-errata/2014-October/004595.html

OEL6
x86_64
wget-1.12-5.el6_6.1

i386
wget-1.12-5.el6_6.1

OEL7
x86_64
wget-1.14-10.el7_0.1

140599 - Red Hat Enterprise Linux RHSA-2014-1764 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
RHSA-2014-1764

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1764.html

RHEL6WS
x86_64
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

i386
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

RHEL6D
x86_64
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

i386
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

RHEL7D
x86_64
wget-debuginfo-1.14-10.el7_0.1
wget-1.14-10.el7_0.1

RHEL7WS
x86_64
wget-debuginfo-1.14-10.el7_0.1
wget-1.14-10.el7_0.1

RHEL6S
x86_64
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

i386
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

RHEL7S
x86_64
wget-debuginfo-1.14-10.el7_0.1
wget-1.14-10.el7_0.1

174572 - Scientific Linux Security ERRATA Moderate: wget on SL6.x, SL7.x i386/x86_64 (1411-207)

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

Risk Level: High

CVE: CVE-2014-4877

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: wget on SL6.x, SL7.x i386/x86_64 (1411-207)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=207

SL7
x86_64
wget-debuginfo-1.14-10.el7_0.1
wget-1.14-10.el7_0.1

SL6
x86_64
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

i386
wget-debuginfo-1.12-5.el6_6.1
wget-1.12-5.el6_6.1

174573 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x i386/x86_64 (1411-720)

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

Risk Level: High

CVE: CVE-2014-6457, CVE-2014-6468, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558, CVE-2014-6562

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: java-1.8.0-openjdk on SL6.x i386/x86_64 (1411-720)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=720

SL6
noarch
java-1.8.0-openjdk-javadoc-1.8.0.25-1.b17.el6

x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-headless-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-src-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-devel-1.8.0.25-1.b17.el6

java-1.8.0-openjdk-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-demo-1.8.0.25-1.b17.el6

i386
java-1.8.0-openjdk-debuginfo-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-headless-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-src-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-devel-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-1.8.0.25-1.b17.el6
java-1.8.0-openjdk-demo-1.8.0.25-1.b17.el6

88645 - Slackware Linux 14.1 SSA:2014-307-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6464, CVE-2014-6469, CVE-2014-6491, CVE-2014-6494, CVE-2014-6496, CVE-2014-6500, CVE-2014-6507, CVE-2014-6555, CVE-2014-6559

Description

The scan detected that the host is missing the following update:
SSA:2014-307-01

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=2014&m=slackware-security.386696

Slackware 14.1
x86_64
mariadb-5.5.40-x86_64-1

174575 - Scientific Linux Security ERRATA Moderate: krb5 on SL6.x i386/x86_64 (1411-987)

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

Risk Level: High

CVE: CVE-2013-1418, CVE-2013-6800, CVE-2014-4341, CVE-2014-4342, CVE-2014-4343, CVE-2014-4344, CVE-2014-4345

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: krb5 on SL6.x i386/x86_64 (1411-987)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=987

SL6
x86_64
krb5-libs-1.10.3-33.el6
krb5-pkinit-openssl-1.10.3-33.el6
krb5-server-1.10.3-33.el6
krb5-debuginfo-1.10.3-33.el6
krb5-workstation-1.10.3-33.el6
krb5-devel-1.10.3-33.el6

krb5-server-ldap-1.10.3-33.el6

i386
krb5-libs-1.10.3-33.el6
krb5-pkinit-openssl-1.10.3-33.el6
krb5-server-1.10.3-33.el6
krb5-debuginfo-1.10.3-33.el6
krb5-workstation-1.10.3-33.el6
krb5-devel-1.10.3-33.el6
krb5-server-ldap-1.10.3-33.el6

17335 - Solaris AnswerBook2 Unauthorized Admin Access

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

Risk Level: High

CVE: CVE-2000-0696

Description

An unauthorized admin access vulnerability exists within the Sun Solaris AnswerBook2 documentation server that allows for an attacker to add administrative users to the AnswerBook2 user database.

Observation

The Sun Solaris AnswerBook2 documentation server provides web-based documentation services. The AnswerBook2 (ab2) server allows for remote administration of the AnswerBook2 service. The AnswerBook2 administration interface includes the CGI program /cgi-bin/admin/admin that allows for any user to create administrative accounts within the AnswerBook2 user database.

Vulnerable Systems:

dwhttpd 1.2.X - 1.4.2
Solaris 2.6 - 2.8

For more information see:

Sun Alert Notification 23412:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-23412-1

BID 1554:
http://online.securityfocus.com/bid/1554

43149 - HP-UX 11.X PHKL_44170 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
PHKL_44170

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHKL_44170

">patch description

HP-UX 11.31 (NA)

OS-Core.CORE2-KRN,fr=B.11.31,fa=HP-UX_B.11.31_PA,v=HP
ProgSupport.C2-INC,fr=B.11.31,fa=HP-UX_B.11.31_PA,v=HP
ProgSupport.PAUX-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
OS-Core.CORE2-KRN,fr=B.11.31,fa=HP-UX_B.11.31_IA,v=HP
OS-Core.ADMN-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
ProgSupport.C-INC,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
ProgSupport.C2-INC,fr=B.11.31,fa=HP-UX_B.11.31_IA,v=HP
OS-Core.KERN-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP
OS-Core.CORE-ENG-A-MAN,fr=B.11.31,fa=HP-UX_B.11.31_IA/PA,v=HP

58987 - Debian Linux 7.0 DSA-3064-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

The scan detected that the host is missing the following update:
DSA-3064-1

Observation

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

http://www.debian.org/security/2014/dsa-3064

Debian 7.0
all
php5_5.4.34-0+deb7u1

58988 - Debian Linux 7.0 DSA-3061-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1585, CVE-2014-1586

Description

The scan detected that the host is missing the following update:
DSA-3061-1

Observation

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

http://www.debian.org/security/2014/dsa-3061

Debian 7.0
all
icedove_31.2.0-1~deb7u1

85815 - CentOS 6, 7 CESA-2014-1767 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
CESA-2014-1767

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-October/020726.html
http://lists.centos.org/pipermail/centos-announce/2014-October/020723.html

CentOS 7
x86_64
php-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-fpm-5.4.16-23.el7_0.3
php-mysqlnd-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-mbstring-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-devel-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-embedded-5.4.16-23.el7_0.3
php-pgsql-5.4.16-23.el7_0.3
php-enchant-5.4.16-23.el7_0.3
php-pspell-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3
php-dba-5.4.16-23.el7_0.3
php-intl-5.4.16-23.el7_0.3
php-snmp-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-common-5.4.16-23.el7_0.3
php-bcmath-5.4.16-23.el7_0.3
php-pdo-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3

CentOS 6
i686
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6

php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

x86_64
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

85816 - CentOS 5 CESA-2014-1768 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
CESA-2014-1768

Observation

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

For more information see:

http://lists.centos.org/pipermail/centos-announce/2014-October/020724.html

CentOS 5
x86_64
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

i386
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

88643 - Slackware Linux 14.0, 14.1 SSA:2014-307-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670

Description

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

SSA:2014-307-03

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=2014&m=slackware-security.403317

Slackware 14.0
x86_64
php-5.4.34-x86_64-1

Slackware 14.1
x86_64
php-5.4.34-x86_64-1

91648 - Oracle Enterprise Linux ELSA-2014-1767 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
ELSA-2014-1767

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004597.html
http://oss.oracle.com/pipermail/el-errata/2014-October/004598.html

OEL6
x86_64
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6

php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

i386
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

OEL7
x86_64
php-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-fpm-5.4.16-23.el7_0.3
php-mysqlnd-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-mbstring-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-devel-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-embedded-5.4.16-23.el7_0.3
php-pgsql-5.4.16-23.el7_0.3
php-enchant-5.4.16-23.el7_0.3
php-pspell-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3
php-dba-5.4.16-23.el7_0.3
php-intl-5.4.16-23.el7_0.3
php-snmp-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-common-5.4.16-23.el7_0.3
php-bcmath-5.4.16-23.el7_0.3

php-pdo-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3

91651 - Oracle Enterprise Linux ELSA-2014-3086 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3181, CVE-2014-3185, CVE-2014-3535, CVE-2014-3611

Description

The scan detected that the host is missing the following update:
ELSA-2014-3086

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004609.html
http://oss.oracle.com/pipermail/el-errata/2014-November/004608.html

OEL6
x86_64
kernel-uek-debug-2.6.32-400.36.10.el6uek
mlnx_en-2.6.32-400.36.10.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.36.10.el6uekdebug-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.36.10.el6uek
kernel-uek-debug-devel-2.6.32-400.36.10.el6uek
kernel-uek-doc-2.6.32-400.36.10.el6uek
kernel-uek-2.6.32-400.36.10.el6uek
kernel-uek-headers-2.6.32-400.36.10.el6uek
mlnx_en-2.6.32-400.36.10.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.36.10.el6uek
ofa-2.6.32-400.36.10.el6uek-1.5.1-4.0.58

i386
kernel-uek-debug-2.6.32-400.36.10.el6uek
mlnx_en-2.6.32-400.36.10.el6uekdebug-1.5.7-0.1
ofa-2.6.32-400.36.10.el6uekdebug-1.5.1-4.0.58
kernel-uek-firmware-2.6.32-400.36.10.el6uek
kernel-uek-debug-devel-2.6.32-400.36.10.el6uek
kernel-uek-doc-2.6.32-400.36.10.el6uek
kernel-uek-2.6.32-400.36.10.el6uek
kernel-uek-headers-2.6.32-400.36.10.el6uek
mlnx_en-2.6.32-400.36.10.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.36.10.el6uek
ofa-2.6.32-400.36.10.el6uek-1.5.1-4.0.58

OEL5
x86_64
mlnx_en-2.6.32-400.36.10.el5uekdebug-1.5.7-2
kernel-uek-headers-2.6.32-400.36.10.el5uek
kernel-uek-debug-2.6.32-400.36.10.el5uek
ofa-2.6.32-400.36.10.el5uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.36.10.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.36.10.el5uek
kernel-uek-devel-2.6.32-400.36.10.el5uek
kernel-uek-2.6.32-400.36.10.el5uek
kernel-uek-doc-2.6.32-400.36.10.el5uek

kernel-uek-firmware-2.6.32-400.36.10.el5uek
ofa-2.6.32-400.36.10.el5uekdebug-1.5.1-4.0.58

i386
mlnx_en-2.6.32-400.36.10.el5uekdebug-1.5.7-2
kernel-uek-headers-2.6.32-400.36.10.el5uek
kernel-uek-debug-2.6.32-400.36.10.el5uek
ofa-2.6.32-400.36.10.el5uek-1.5.1-4.0.58
mlnx_en-2.6.32-400.36.10.el5uek-1.5.7-2
kernel-uek-debug-devel-2.6.32-400.36.10.el5uek
kernel-uek-devel-2.6.32-400.36.10.el5uek
kernel-uek-2.6.32-400.36.10.el5uek
kernel-uek-doc-2.6.32-400.36.10.el5uek
kernel-uek-firmware-2.6.32-400.36.10.el5uek
ofa-2.6.32-400.36.10.el5uekdebug-1.5.1-4.0.58

91654 - Oracle Enterprise Linux ELSA-2014-1768 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
ELSA-2014-1768

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004599.html

OEL5
x86_64
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

i386
php53-mysql-5.3.3-26.el5_11

php53-imap-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

140595 - Red Hat Enterprise Linux RHSA-2014-1767 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
RHSA-2014-1767

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1767.html

RHEL6WS
x86_64
php-gd-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6

i386
php-gd-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6

php-mysql-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6

RHEL6D
x86_64
php-debuginfo-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6

RHEL7D
x86_64
php-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-debuginfo-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-fpm-5.4.16-23.el7_0.3
php-mysqlnd-5.4.16-23.el7_0.3
php-mbstring-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-devel-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3
php-embedded-5.4.16-23.el7_0.3
php-pgsql-5.4.16-23.el7_0.3
php-enchant-5.4.16-23.el7_0.3
php-pspell-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3
php-dba-5.4.16-23.el7_0.3
php-intl-5.4.16-23.el7_0.3
php-snmp-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-common-5.4.16-23.el7_0.3
php-bcmath-5.4.16-23.el7_0.3
php-pdo-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3

RHEL7WS
x86_64
php-pgsql-5.4.16-23.el7_0.3
php-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-debuginfo-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-pdo-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3

php-common-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3

RHEL6S
x86_64
php-gd-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6

i386
php-gd-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6

RHEL7S
x86_64
php-pgsql-5.4.16-23.el7_0.3
php-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-debuginfo-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-pdo-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3
php-common-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3

140596 - Red Hat Enterprise Linux RHSA-2014-1766 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1571, CVE-2014-0207, CVE-2014-0237, CVE-2014-0238, CVE-2014-2497, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3515, CVE-2014-3538, CVE-2014-3587, CVE-2014-3597, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710, CVE-2014-4049, CVE-2014-4670, CVE-2014-4698, CVE-2014-4721, CVE-2014-

5120

Description

The scan detected that the host is missing the following update:
RHSA-2014-1766

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1766.html

RHEL6WS
x86_64
php55-php-gd-5.5.6-13.el6
php55-php-5.5.6-13.el6
php55-php-odbc-5.5.6-13.el6
php55-php-common-5.5.6-13.el6
php55-php-cli-5.5.6-13.el6
php55-php-ldap-5.5.6-13.el6
php55-php-tidy-5.5.6-13.el6
php55-php-pdo-5.5.6-13.el6
php55-php-dba-5.5.6-13.el6
php55-php-fpm-5.5.6-13.el6
php55-php-mysqlnd-5.5.6-13.el6
php55-php-soap-5.5.6-13.el6
php55-php-snmp-5.5.6-13.el6
php55-php-debuginfo-5.5.6-13.el6
php55-php-xml-5.5.6-13.el6
php55-php-opcache-5.5.6-13.el6
php55-php-bcmath-5.5.6-13.el6
php55-php-pspell-5.5.6-13.el6
php55-php-mbstring-5.5.6-13.el6
php55-php-intl-5.5.6-13.el6
php55-php-xmlrpc-5.5.6-13.el6
php55-php-gmp-5.5.6-13.el6
php55-php-imap-5.5.6-13.el6
php55-php-pgsql-5.5.6-13.el6
php55-php-enchant-5.5.6-13.el6
php55-php-devel-5.5.6-13.el6
php55-php-recode-5.5.6-13.el6
php55-php-process-5.5.6-13.el6

RHEL7WS
x86_64
php55-php-pgsql-5.5.6-13.el7
php55-php-snmp-5.5.6-13.el7
php55-php-odbc-5.5.6-13.el7
php55-php-common-5.5.6-13.el7
php55-php-recode-5.5.6-13.el7
php55-php-mbstring-5.5.6-13.el7
php55-php-enchant-5.5.6-13.el7
php55-php-ldap-5.5.6-13.el7
php55-php-debuginfo-5.5.6-13.el7
php55-php-gmp-5.5.6-13.el7
php55-php-xmlrpc-5.5.6-13.el7
php55-php-cli-5.5.6-13.el7
php55-php-intl-5.5.6-13.el7
php55-php-pspell-5.5.6-13.el7

php55-php-devel-5.5.6-13.el7
php55-php-xml-5.5.6-13.el7
php55-php-5.5.6-13.el7
php55-php-bcmath-5.5.6-13.el7
php55-php-opcache-5.5.6-13.el7
php55-php-dba-5.5.6-13.el7
php55-php-fpm-5.5.6-13.el7
php55-php-mysqlnd-5.5.6-13.el7
php55-php-soap-5.5.6-13.el7
php55-php-process-5.5.6-13.el7
php55-php-pdo-5.5.6-13.el7
php55-php-gd-5.5.6-13.el7

RHEL6S
x86_64
php55-php-gd-5.5.6-13.el6
php55-php-5.5.6-13.el6
php55-php-odbc-5.5.6-13.el6
php55-php-common-5.5.6-13.el6
php55-php-cli-5.5.6-13.el6
php55-php-ldap-5.5.6-13.el6
php55-php-tidy-5.5.6-13.el6
php55-php-pdo-5.5.6-13.el6
php55-php-dba-5.5.6-13.el6
php55-php-fpm-5.5.6-13.el6
php55-php-mysqlnd-5.5.6-13.el6
php55-php-soap-5.5.6-13.el6
php55-php-snmp-5.5.6-13.el6
php55-php-debuginfo-5.5.6-13.el6
php55-php-xml-5.5.6-13.el6
php55-php-opcache-5.5.6-13.el6
php55-php-bcmath-5.5.6-13.el6
php55-php-pspell-5.5.6-13.el6
php55-php-mbstring-5.5.6-13.el6
php55-php-intl-5.5.6-13.el6
php55-php-xmlrpc-5.5.6-13.el6
php55-php-gmp-5.5.6-13.el6
php55-php-imap-5.5.6-13.el6
php55-php-pgsql-5.5.6-13.el6
php55-php-enchant-5.5.6-13.el6
php55-php-devel-5.5.6-13.el6
php55-php-recode-5.5.6-13.el6
php55-php-process-5.5.6-13.el6

RHEL7S
x86_64
php55-php-pgsql-5.5.6-13.el7
php55-php-snmp-5.5.6-13.el7
php55-php-odbc-5.5.6-13.el7
php55-php-common-5.5.6-13.el7
php55-php-recode-5.5.6-13.el7
php55-php-mbstring-5.5.6-13.el7
php55-php-enchant-5.5.6-13.el7
php55-php-ldap-5.5.6-13.el7
php55-php-debuginfo-5.5.6-13.el7
php55-php-gmp-5.5.6-13.el7
php55-php-xmlrpc-5.5.6-13.el7
php55-php-cli-5.5.6-13.el7
php55-php-intl-5.5.6-13.el7
php55-php-pspell-5.5.6-13.el7

php55-php-devel-5.5.6-13.el7
php55-php-xml-5.5.6-13.el7
php55-php-5.5.6-13.el7
php55-php-bcmath-5.5.6-13.el7
php55-php-opcache-5.5.6-13.el7
php55-php-dba-5.5.6-13.el7
php55-php-fpm-5.5.6-13.el7
php55-php-mysqlnd-5.5.6-13.el7
php55-php-soap-5.5.6-13.el7
php55-php-process-5.5.6-13.el7
php55-php-pdo-5.5.6-13.el7
php55-php-gd-5.5.6-13.el7

140597 - Red Hat Enterprise Linux RHSA-2014-1801 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3675, CVE-2014-3676, CVE-2014-3677

Description

The scan detected that the host is missing the following update:
RHSA-2014-1801

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1801.html

RHEL7WS
x86_64
shim-0.7-8.el7_0
shim-debuginfo-0.7-8.el7_0
mokutil-0.7-8.el7_0
shim-unsigned-0.7-8.el7_0

RHEL7D
x86_64
shim-0.7-8.el7_0
shim-debuginfo-0.7-8.el7_0
mokutil-0.7-8.el7_0
shim-unsigned-0.7-8.el7_0

RHEL7S
x86_64
shim-0.7-8.el7_0
shim-debuginfo-0.7-8.el7_0
mokutil-0.7-8.el7_0
shim-unsigned-0.7-8.el7_0

140598 - Red Hat Enterprise Linux RHSA-2014-1765 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1571, CVE-2013-6712, CVE-2013-7345, CVE-2014-0207, CVE-2014-0237, CVE-2014-0238, CVE-2014-1943, CVE-2014-2270, CVE-2014-2497, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3515, CVE-2014-3538, CVE-2014-3587, CVE-2014-3597, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710, CVE-2014-

4049, CVE-2014-4670, CVE-2014-4698, CVE-2014-4721, CVE-2014-5120

Description

The scan detected that the host is missing the following update:
RHSA-2014-1765

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1765.html

RHEL6WS
x86_64
php54-php-5.4.16-22.el6
php54-php-soap-5.4.16-22.el6
php54-php-enchant-5.4.16-22.el6
php54-php-mbstring-5.4.16-22.el6
php54-php-odbc-5.4.16-22.el6
php54-php-pdo-5.4.16-22.el6
php54-php-mysqlnd-5.4.16-22.el6
php54-php-snmp-5.4.16-22.el6
php54-php-xml-5.4.16-22.el6
php54-php-ldap-5.4.16-22.el6
php54-php-devel-5.4.16-22.el6
php54-php-imap-5.4.16-22.el6
php54-php-xmlrpc-5.4.16-22.el6
php54-php-tidy-5.4.16-22.el6
php54-php-bcmath-5.4.16-22.el6
php54-php-gd-5.4.16-22.el6
php54-php-fpm-5.4.16-22.el6
php54-php-cli-5.4.16-22.el6
php54-php-recode-5.4.16-22.el6
php54-php-process-5.4.16-22.el6
php54-php-pspell-5.4.16-22.el6
php54-php-intl-5.4.16-22.el6
php54-php-dba-5.4.16-22.el6
php54-php-debuginfo-5.4.16-22.el6
php54-php-pgsql-5.4.16-22.el6
php54-php-common-5.4.16-22.el6

RHEL7WS
x86_64
php54-php-snmp-5.4.16-22.el7
php54-php-recode-5.4.16-22.el7
php54-php-enchant-5.4.16-22.el7
php54-php-cli-5.4.16-22.el7
php54-php-fpm-5.4.16-22.el7
php54-php-ldap-5.4.16-22.el7
php54-php-bcmath-5.4.16-22.el7
php54-php-pdo-5.4.16-22.el7
php54-php-mbstring-5.4.16-22.el7
php54-php-gd-5.4.16-22.el7
php54-php-pspell-5.4.16-22.el7
php54-php-dba-5.4.16-22.el7
php54-php-xmlrpc-5.4.16-22.el7
php54-php-devel-5.4.16-22.el7
php54-php-odbc-5.4.16-22.el7
php54-php-intl-5.4.16-22.el7

php54-php-common-5.4.16-22.el7
php54-php-soap-5.4.16-22.el7
php54-php-mysqlnd-5.4.16-22.el7
php54-php-xml-5.4.16-22.el7
php54-php-debuginfo-5.4.16-22.el7
php54-php-5.4.16-22.el7
php54-php-process-5.4.16-22.el7
php54-php-pgsql-5.4.16-22.el7

RHEL6S
x86_64
php54-php-5.4.16-22.el6
php54-php-soap-5.4.16-22.el6
php54-php-enchant-5.4.16-22.el6
php54-php-mbstring-5.4.16-22.el6
php54-php-odbc-5.4.16-22.el6
php54-php-pdo-5.4.16-22.el6
php54-php-mysqlnd-5.4.16-22.el6
php54-php-snmp-5.4.16-22.el6
php54-php-xml-5.4.16-22.el6
php54-php-ldap-5.4.16-22.el6
php54-php-devel-5.4.16-22.el6
php54-php-imap-5.4.16-22.el6
php54-php-xmlrpc-5.4.16-22.el6
php54-php-tidy-5.4.16-22.el6
php54-php-bcmath-5.4.16-22.el6
php54-php-gd-5.4.16-22.el6
php54-php-fpm-5.4.16-22.el6
php54-php-cli-5.4.16-22.el6
php54-php-recode-5.4.16-22.el6
php54-php-process-5.4.16-22.el6
php54-php-pspell-5.4.16-22.el6
php54-php-intl-5.4.16-22.el6
php54-php-dba-5.4.16-22.el6
php54-php-debuginfo-5.4.16-22.el6
php54-php-pgsql-5.4.16-22.el6
php54-php-common-5.4.16-22.el6

RHEL7S
x86_64
php54-php-snmp-5.4.16-22.el7
php54-php-recode-5.4.16-22.el7
php54-php-enchant-5.4.16-22.el7
php54-php-cli-5.4.16-22.el7
php54-php-fpm-5.4.16-22.el7
php54-php-ldap-5.4.16-22.el7
php54-php-bcmath-5.4.16-22.el7
php54-php-pdo-5.4.16-22.el7
php54-php-mbstring-5.4.16-22.el7
php54-php-gd-5.4.16-22.el7
php54-php-pspell-5.4.16-22.el7
php54-php-dba-5.4.16-22.el7
php54-php-xmlrpc-5.4.16-22.el7
php54-php-devel-5.4.16-22.el7
php54-php-odbc-5.4.16-22.el7
php54-php-intl-5.4.16-22.el7
php54-php-common-5.4.16-22.el7
php54-php-soap-5.4.16-22.el7
php54-php-mysqlnd-5.4.16-22.el7
php54-php-xml-5.4.16-22.el7

php54-php-debuginfo-5.4.16-22.el7
php54-php-5.4.16-22.el7
php54-php-process-5.4.16-22.el7
php54-php-pgsql-5.4.16-22.el7

140601 - Red Hat Enterprise Linux RHSA-2014-1768 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
RHSA-2014-1768

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1768.html

RHEL5D
x86_64
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

i386
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11

php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

RHEL5S
x86_64
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

i386
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

142478 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1331-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1331-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-10/msg00035.html

SuSE Linux 13.1
i586
libopenssl1_0_0-1.0.1j-11.56.1
libopenssl-devel-1.0.1j-11.56.1
openssl-1.0.1j-11.56.1
openssl-debuginfo-1.0.1j-11.56.1
libopenssl1_0_0-debuginfo-1.0.1j-11.56.1
openssl-debugsource-1.0.1j-11.56.1

x86_64
openssl-doc-1.0.1j-11.56.1
libopenssl-devel-32bit-1.0.1j-11.56.1
libopenssl1_0_0-32bit-1.0.1j-11.56.1
libopenssl1_0_0-debuginfo-32bit-1.0.1j-11.56.1

SuSE Linux 12.3
i586
libopenssl1_0_0-1.0.1j-1.68.1
openssl-debugsource-1.0.1j-1.68.1
libopenssl1_0_0-debuginfo-1.0.1j-1.68.1
openssl-debuginfo-1.0.1j-1.68.1
openssl-1.0.1j-1.68.1
libopenssl-devel-1.0.1j-1.68.1

x86_64
libopenssl1_0_0-debuginfo-32bit-1.0.1j-1.68.1
openssl-doc-1.0.1j-1.68.1
libopenssl-devel-32bit-1.0.1j-1.68.1
libopenssl1_0_0-32bit-1.0.1j-1.68.1

142479 - SuSE Linux 12.3 openSUSE-SU-2014:1343-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1585, CVE-2014-1586

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1343-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00000.html

SuSE Linux 12.3
i586
MozillaThunderbird-debugsource-31.2.0-61.63.1
MozillaThunderbird-31.2.0-61.63.1
MozillaThunderbird-debuginfo-31.2.0-61.63.1
MozillaThunderbird-buildsymbols-31.2.0-61.63.1
MozillaThunderbird-devel-31.2.0-61.63.1
MozillaThunderbird-translations-common-31.2.0-61.63.1
MozillaThunderbird-translations-other-31.2.0-61.63.1

142482 - SuSE Linux 13.1 openSUSE-SU-2014:1346-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1585, CVE-2014-1586

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1346-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00003.html

SuSE Linux 13.1
i586
MozillaThunderbird-31.2.0-70.35.2
MozillaThunderbird-debugsource-31.2.0-70.35.2
MozillaThunderbird-devel-31.2.0-70.35.2
MozillaThunderbird-debuginfo-31.2.0-70.35.2
MozillaThunderbird-translations-common-31.2.0-70.35.2
MozillaThunderbird-buildsymbols-31.2.0-70.35.2
MozillaThunderbird-translations-other-31.2.0-70.35.2

174571 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86_64 (1411-581)

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583

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 (1411-581)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=581

SL7
x86_64
xulrunner-debuginfo-31.2.0-1.el7_0
firefox-debuginfo-31.2.0-3.el7_0
xulrunner-31.2.0-1.el7_0
firefox-31.2.0-3.el7_0
xulrunner-devel-31.2.0-1.el7_0

SL5
x86_64
firefox-debuginfo-31.2.0-3.el5_11
firefox-31.2.0-3.el5_11

i386
firefox-debuginfo-31.2.0-3.el5_11
firefox-31.2.0-3.el5_11

SL6
x86_64
firefox-31.2.0-3.el6_6
firefox-debuginfo-31.2.0-3.el6_6

i386
firefox-31.2.0-3.el6_6
firefox-debuginfo-31.2.0-3.el6_6

174578 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1411-857)

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

Risk Level: High

CVE: CVE-2014-1574, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1411-857)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=857

SL6
x86_64
thunderbird-31.2.0-3.el6_6
thunderbird-debuginfo-31.2.0-3.el6_6

i386
thunderbird-31.2.0-3.el6_6
thunderbird-debuginfo-31.2.0-3.el6_6

174580 - Scientific Linux Security ERRATA Important: php on SL6.x, SL7.x i386/x86_64 (1411-79)

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: php on SL6.x, SL7.x i386/x86_64 (1411-79)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=79

SL7
x86_64
php-5.4.16-23.el7_0.3
php-cli-5.4.16-23.el7_0.3
php-debuginfo-5.4.16-23.el7_0.3
php-xml-5.4.16-23.el7_0.3
php-fpm-5.4.16-23.el7_0.3
php-mysqlnd-5.4.16-23.el7_0.3
php-mbstring-5.4.16-23.el7_0.3
php-gd-5.4.16-23.el7_0.3
php-process-5.4.16-23.el7_0.3
php-soap-5.4.16-23.el7_0.3
php-ldap-5.4.16-23.el7_0.3
php-devel-5.4.16-23.el7_0.3
php-odbc-5.4.16-23.el7_0.3
php-embedded-5.4.16-23.el7_0.3
php-pgsql-5.4.16-23.el7_0.3
php-enchant-5.4.16-23.el7_0.3
php-pspell-5.4.16-23.el7_0.3
php-xmlrpc-5.4.16-23.el7_0.3
php-dba-5.4.16-23.el7_0.3
php-intl-5.4.16-23.el7_0.3
php-snmp-5.4.16-23.el7_0.3
php-mysql-5.4.16-23.el7_0.3
php-common-5.4.16-23.el7_0.3
php-bcmath-5.4.16-23.el7_0.3
php-pdo-5.4.16-23.el7_0.3
php-recode-5.4.16-23.el7_0.3

SL6
x86_64
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6

php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

i386
php-snmp-5.3.3-40.el6_6
php-embedded-5.3.3-40.el6_6
php-gd-5.3.3-40.el6_6
php-mysql-5.3.3-40.el6_6
php-tidy-5.3.3-40.el6_6
php-odbc-5.3.3-40.el6_6
php-debuginfo-5.3.3-40.el6_6
php-mbstring-5.3.3-40.el6_6
php-process-5.3.3-40.el6_6
php-dba-5.3.3-40.el6_6
php-pspell-5.3.3-40.el6_6
php-soap-5.3.3-40.el6_6
php-devel-5.3.3-40.el6_6
php-pgsql-5.3.3-40.el6_6
php-common-5.3.3-40.el6_6
php-recode-5.3.3-40.el6_6
php-bcmath-5.3.3-40.el6_6
php-imap-5.3.3-40.el6_6
php-fpm-5.3.3-40.el6_6
php-intl-5.3.3-40.el6_6
php-5.3.3-40.el6_6
php-cli-5.3.3-40.el6_6
php-pdo-5.3.3-40.el6_6
php-xmlrpc-5.3.3-40.el6_6
php-zts-5.3.3-40.el6_6
php-ldap-5.3.3-40.el6_6
php-enchant-5.3.3-40.el6_6
php-xml-5.3.3-40.el6_6

174584 - Scientific Linux Security ERRATA Important: php53 on SL5.x i386/x86_64 (1411-336)

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

Risk Level: High

CVE: CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3710

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: php53 on SL5.x i386/x86_64 (1411-336)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=336

SL5
x86_64
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

i386
php53-mysql-5.3.3-26.el5_11
php53-imap-5.3.3-26.el5_11
php53-process-5.3.3-26.el5_11
php53-bcmath-5.3.3-26.el5_11
php53-pdo-5.3.3-26.el5_11
php53-dba-5.3.3-26.el5_11
php53-xmlrpc-5.3.3-26.el5_11
php53-devel-5.3.3-26.el5_11
php53-pspell-5.3.3-26.el5_11
php53-mbstring-5.3.3-26.el5_11
php53-5.3.3-26.el5_11
php53-gd-5.3.3-26.el5_11
php53-snmp-5.3.3-26.el5_11
php53-odbc-5.3.3-26.el5_11
php53-pgsql-5.3.3-26.el5_11
php53-intl-5.3.3-26.el5_11
php53-debuginfo-5.3.3-26.el5_11
php53-ldap-5.3.3-26.el5_11
php53-soap-5.3.3-26.el5_11
php53-cli-5.3.3-26.el5_11
php53-common-5.3.3-26.el5_11
php53-xml-5.3.3-26.el5_11

85818 - CentOS 7 CESA-2014-1724 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-4653, CVE-2014-5077

Description

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

CESA-2014-1724

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-October/020710.html

CentOS 7
noarch
kernel-abi-whitelists-3.10.0-123.9.2.el7
kernel-doc-3.10.0-123.9.2.el7

x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
kernel-tools-libs-devel-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
python-perf-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7

91647 - Oracle Enterprise Linux ELSA-2014-3085 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3181, CVE-2014-3185, CVE-2014-3611

Description

The scan detected that the host is missing the following update:
ELSA-2014-3085

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004590.html
http://oss.oracle.com/pipermail/el-errata/2014-October/004589.html

OEL6
x86_64
kernel-uek-firmware-2.6.39-400.215.12.el6uek
kernel-uek-2.6.39-400.215.12.el6uek
kernel-uek-debug-2.6.39-400.215.12.el6uek
kernel-uek-devel-2.6.39-400.215.12.el6uek
kernel-uek-debug-devel-2.6.39-400.215.12.el6uek
kernel-uek-doc-2.6.39-400.215.12.el6uek

i386
kernel-uek-debug-devel-2.6.39-400.215.12.el6uek
kernel-uek-2.6.39-400.215.12.el6uek
kernel-uek-devel-2.6.39-400.215.12.el6uek
kernel-uek-debug-2.6.39-400.215.12.el6uek
kernel-uek-firmware-2.6.39-400.215.12.el6uek

kernel-uek-doc-2.6.39-400.215.12.el6uek

OEL5
x86_64
kernel-uek-debug-2.6.39-400.215.12.el5uek
kernel-uek-firmware-2.6.39-400.215.12.el5uek
kernel-uek-debug-devel-2.6.39-400.215.12.el5uek
kernel-uek-doc-2.6.39-400.215.12.el5uek
kernel-uek-devel-2.6.39-400.215.12.el5uek
kernel-uek-2.6.39-400.215.12.el5uek

i386
kernel-uek-firmware-2.6.39-400.215.12.el5uek
kernel-uek-doc-2.6.39-400.215.12.el5uek
kernel-uek-debug-devel-2.6.39-400.215.12.el5uek
kernel-uek-debug-2.6.39-400.215.12.el5uek
kernel-uek-2.6.39-400.215.12.el5uek
kernel-uek-devel-2.6.39-400.215.12.el5uek

91650 - Oracle Enterprise Linux ELSA-2014-1724 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-4653, CVE-2014-5077

Description

The scan detected that the host is missing the following update:
ELSA-2014-1724

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004581.html

OEL7
x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
kernel-tools-libs-devel-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
python-perf-3.10.0-123.9.2.el7
kernel-abi-whitelists-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
kernel-doc-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7

91653 - Oracle Enterprise Linux ELSA-2014-3084 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3181, CVE-2014-3185, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646

Description

The scan detected that the host is missing the following update:
ELSA-2014-3084

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-October/004588.html
http://oss.oracle.com/pipermail/el-errata/2014-October/004593.html

OEL6
x86_64
kernel-uek-debug-devel-3.8.13-44.1.4.el6uek
kernel-uek-3.8.13-44.1.4.el6uek
kernel-uek-devel-3.8.13-44.1.4.el6uek
kernel-uek-debug-3.8.13-44.1.4.el6uek
kernel-uek-firmware-3.8.13-44.1.4.el6uek
dtrace-modules-3.8.13-44.1.4.el6uek-0.4.3-4.el6
kernel-uek-doc-3.8.13-44.1.4.el6uek

OEL7
x86_64
kernel-uek-doc-3.8.13-44.1.4.el7uek
kernel-uek-devel-3.8.13-44.1.4.el7uek
kernel-uek-debug-3.8.13-44.1.4.el7uek
kernel-uek-debug-devel-3.8.13-44.1.4.el7uek
kernel-uek-3.8.13-44.1.4.el7uek
kernel-uek-firmware-3.8.13-44.1.4.el7uek
dtrace-modules-3.8.13-44.1.4.el7uek-0.4.3-4.el7

174577 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1411-1615)

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

Risk Level: Medium

CVE: CVE-2013-2596, CVE-2013-4483, CVE-2014-0181, CVE-2014-3122, CVE-2014-3601, CVE-2014-4608, CVE-2014-4653, CVE-2014-4654, CVE-2014-4655, CVE-2014-5045, CVE-2014-5077

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL6.x i386/x86_64 (1411-1615)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1615

SL6
noarch
kernel-firmware-2.6.32-504.el6
kernel-doc-2.6.32-504.el6
kernel-abi-whitelists-2.6.32-504.el6

x86_64
perf-2.6.32-504.el6
kernel-debuginfo-common-x86_64-2.6.32-504.el6
kernel-debug-devel-2.6.32-504.el6

kernel-debug-debuginfo-2.6.32-504.el6
kernel-devel-2.6.32-504.el6
perf-debuginfo-2.6.32-504.el6
kernel-debug-2.6.32-504.el6
python-perf-2.6.32-504.el6
kernel-2.6.32-504.el6
kernel-headers-2.6.32-504.el6
python-perf-debuginfo-2.6.32-504.el6
kernel-debuginfo-2.6.32-504.el6

i386
perf-2.6.32-504.el6
kernel-headers-2.6.32-504.el6
kernel-debug-devel-2.6.32-504.el6
kernel-debug-debuginfo-2.6.32-504.el6
kernel-debuginfo-common-i686-2.6.32-504.el6
kernel-devel-2.6.32-504.el6
perf-debuginfo-2.6.32-504.el6
kernel-debug-2.6.32-504.el6
python-perf-2.6.32-504.el6
kernel-2.6.32-504.el6
python-perf-debuginfo-2.6.32-504.el6
kernel-debuginfo-2.6.32-504.el6

174579 - Scientific Linux Security ERRATA Moderate: luci on SL6.x i386/x86_64 (1411-1109)

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

Risk Level: Medium

CVE: CVE-2014-3593

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: luci on SL6.x i386/x86_64 (1411-1109)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1109

SL6
x86_64
luci-debuginfo-0.26.0-63.el6
luci-0.26.0-63.el6

i386
luci-debuginfo-0.26.0-63.el6
luci-0.26.0-63.el6

174581 - Scientific Linux Security ERRATA Moderate: X11 client libraries on SL6.x i386/x86_64 (1411-1476)

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

Risk Level: Medium

CVE: CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1991, CVE-2013-1995, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2064, CVE-2013-2066

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: X11 client libraries on SL6.x i386/x86_64 (1411-1476)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1476

SL6
noarch
xorg-x11-xtrans-devel-1.3.4-1.el6
xkeyboard-config-devel-2.11-1.el6
xcb-proto-1.8-3.el6
libX11-common-1.6.0-2.2.el6
xorg-x11-proto-devel-7.7-9.el6
xkeyboard-config-2.11-1.el6
libxcb-doc-1.9.1-2.el6

x86_64
libX11-devel-1.6.0-2.2.el6
libXrandr-1.4.1-2.1.el6
libXi-devel-1.7.2-2.2.el6
libXv-debuginfo-1.0.9-2.1.el6
libXi-1.7.2-2.2.el6
libXvMC-debuginfo-1.0.8-2.1.el6
libXxf86vm-debuginfo-1.1.3-2.1.el6
libXinerama-devel-1.1.3-2.1.el6
libXxf86vm-1.1.3-2.1.el6
libXtst-debuginfo-1.2.2-2.1.el6
libXext-1.3.2-2.1.el6
libXres-devel-1.0.7-2.1.el6
libXcursor-1.1.14-2.1.el6
libX11-1.6.0-2.2.el6
libXrender-0.9.8-2.1.el6
libXrender-devel-0.9.8-2.1.el6
libX11-debuginfo-1.6.0-2.2.el6
libXp-devel-1.0.2-2.1.el6
libXtst-1.2.2-2.1.el6
libXfixes-5.0.1-2.1.el6
libXt-1.1.4-6.1.el6
libxcb-debuginfo-1.9.1-2.el6
libdmx-debuginfo-1.1.3-3.el6
libXres-debuginfo-1.0.7-2.1.el6
libXinerama-debuginfo-1.1.3-2.1.el6
libXcursor-debuginfo-1.1.14-2.1.el6
libXext-debuginfo-1.3.2-2.1.el6
libXvMC-1.0.8-2.1.el6
libXxf86dga-devel-1.1.4-2.1.el6
libdmx-1.1.3-3.el6
libxcb-python-1.9.1-2.el6
libXt-debuginfo-1.1.4-6.1.el6
libXp-debuginfo-1.0.2-2.1.el6
libXv-1.0.9-2.1.el6
libXt-devel-1.1.4-6.1.el6
libXtst-devel-1.2.2-2.1.el6
libXi-debuginfo-1.7.2-2.2.el6

libdmx-devel-1.1.3-3.el6
libXrender-debuginfo-0.9.8-2.1.el6
libXinerama-1.1.3-2.1.el6
libxcb-devel-1.9.1-2.el6
libXfixes-devel-5.0.1-2.1.el6
libXv-devel-1.0.9-2.1.el6
libXext-devel-1.3.2-2.1.el6
libXfixes-debuginfo-5.0.1-2.1.el6
libXrandr-devel-1.4.1-2.1.el6
libXxf86vm-devel-1.1.3-2.1.el6
libXcursor-devel-1.1.14-2.1.el6
libXxf86dga-debuginfo-1.1.4-2.1.el6
libXrandr-debuginfo-1.4.1-2.1.el6
libXp-1.0.2-2.1.el6
libXvMC-devel-1.0.8-2.1.el6
libxcb-1.9.1-2.el6
libXxf86dga-1.1.4-2.1.el6
libXres-1.0.7-2.1.el6

i386
libX11-devel-1.6.0-2.2.el6
libXrandr-1.4.1-2.1.el6
libXi-devel-1.7.2-2.2.el6
libXv-debuginfo-1.0.9-2.1.el6
libXi-1.7.2-2.2.el6
libXvMC-debuginfo-1.0.8-2.1.el6
libXxf86vm-debuginfo-1.1.3-2.1.el6
libXinerama-devel-1.1.3-2.1.el6
libXxf86vm-1.1.3-2.1.el6
libXtst-debuginfo-1.2.2-2.1.el6
libXext-1.3.2-2.1.el6
libXres-devel-1.0.7-2.1.el6
libXcursor-1.1.14-2.1.el6
libX11-1.6.0-2.2.el6
libXrender-0.9.8-2.1.el6
libXrender-devel-0.9.8-2.1.el6
libX11-debuginfo-1.6.0-2.2.el6
libXp-devel-1.0.2-2.1.el6
libXtst-1.2.2-2.1.el6
libXfixes-5.0.1-2.1.el6
libXt-1.1.4-6.1.el6
libxcb-debuginfo-1.9.1-2.el6
libdmx-debuginfo-1.1.3-3.el6
libXres-debuginfo-1.0.7-2.1.el6
libXinerama-debuginfo-1.1.3-2.1.el6
libXcursor-debuginfo-1.1.14-2.1.el6
libXext-debuginfo-1.3.2-2.1.el6
libXvMC-1.0.8-2.1.el6
libXxf86dga-devel-1.1.4-2.1.el6
libdmx-1.1.3-3.el6
libxcb-python-1.9.1-2.el6
libXt-debuginfo-1.1.4-6.1.el6
libXp-debuginfo-1.0.2-2.1.el6
libXv-1.0.9-2.1.el6
libXt-devel-1.1.4-6.1.el6
libXtst-devel-1.2.2-2.1.el6
libXi-debuginfo-1.7.2-2.2.el6
libdmx-devel-1.1.3-3.el6
libXrender-debuginfo-0.9.8-2.1.el6
libXinerama-1.1.3-2.1.el6

libxcb-devel-1.9.1-2.el6
libXfixes-devel-5.0.1-2.1.el6
libXv-devel-1.0.9-2.1.el6
libXext-devel-1.3.2-2.1.el6
libXfixes-debuginfo-5.0.1-2.1.el6
libXrandr-devel-1.4.1-2.1.el6
libXxf86vm-devel-1.1.3-2.1.el6
libXcursor-devel-1.1.14-2.1.el6
libXxf86dga-debuginfo-1.1.4-2.1.el6
libXrandr-debuginfo-1.4.1-2.1.el6
libXp-1.0.2-2.1.el6
libXvMC-devel-1.0.8-2.1.el6
libxcb-1.9.1-2.el6
libXxf86dga-1.1.4-2.1.el6
libXres-1.0.7-2.1.el6

174582 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1411-460)

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

Risk Level: Medium

CVE: CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-4653, CVE-2014-5077

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: kernel on SL7.x x86_64 (1411-460)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=460

SL7
noarch
kernel-abi-whitelists-3.10.0-123.9.2.el7
kernel-doc-3.10.0-123.9.2.el7

x86_64
kernel-tools-libs-3.10.0-123.9.2.el7
kernel-3.10.0-123.9.2.el7
perf-debuginfo-3.10.0-123.9.2.el7
kernel-tools-libs-devel-3.10.0-123.9.2.el7
kernel-debug-debuginfo-3.10.0-123.9.2.el7
kernel-devel-3.10.0-123.9.2.el7
python-perf-3.10.0-123.9.2.el7
kernel-tools-3.10.0-123.9.2.el7
kernel-debuginfo-common-x86_64-3.10.0-123.9.2.el7
kernel-tools-debuginfo-3.10.0-123.9.2.el7
perf-3.10.0-123.9.2.el7
kernel-debug-devel-3.10.0-123.9.2.el7
kernel-headers-3.10.0-123.9.2.el7
kernel-debug-3.10.0-123.9.2.el7
kernel-debuginfo-3.10.0-123.9.2.el7
python-perf-debuginfo-3.10.0-123.9.2.el7

174585 - Scientific Linux Security ERRATA Moderate: glibc on SL6.x i386/x86_64 (1411-1353)

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

Risk Level: Medium

CVE: CVE-2013-4237, CVE-2013-4458

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: glibc on SL6.x i386/x86_64 (1411-1353)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1353

SL6
x86_64
glibc-utils-2.12-1.149.el6
glibc-static-2.12-1.149.el6
glibc-debuginfo-2.12-1.149.el6
glibc-common-2.12-1.149.el6
nscd-2.12-1.149.el6
glibc-headers-2.12-1.149.el6
glibc-debuginfo-common-2.12-1.149.el6
glibc-devel-2.12-1.149.el6
glibc-2.12-1.149.el6

i386
glibc-utils-2.12-1.149.el6
glibc-static-2.12-1.149.el6
glibc-debuginfo-2.12-1.149.el6
glibc-common-2.12-1.149.el6
nscd-2.12-1.149.el6
glibc-headers-2.12-1.149.el6
glibc-debuginfo-common-2.12-1.149.el6
glibc-devel-2.12-1.149.el6
glibc-2.12-1.149.el6

17338 - Cisco IOS ASR901 Crafted IPv4 Packet Denial of Service

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

Risk Level: Medium

CVE: CVE-2014-3293

Description

A vulnerability in some versions of Cisco IOS could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco IOS could lead to a denial of service.

The flaw lies in the handling of crafted IPv4 packets. Successful exploitation by a remote attacker could result in a denial of service condition.

58983 - Debian Linux 7.0 DSA-3059-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8761, CVE-2014-8762, CVE-2014-8763, CVE-2014-8764

Description

The scan detected that the host is missing the following update:
DSA-3059-1

Observation

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

http://www.debian.org/security/2014/dsa-3059

Debian 7.0
all
dokuwiki_0.0.20120125b-2+deb7u1

174576 - Scientific Linux Security ERRATA Moderate: file on SL6.x i386/x86_64 (1411-1742)

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

Risk Level: Medium

CVE: CVE-2012-1571, CVE-2014-0237, CVE-2014-0238, CVE-2014-1943, CVE-2014-2270, CVE-2014-3479, CVE-2014-3480

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: file on SL6.x i386/x86_64 (1411-1742)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1742

SL6
x86_64
file-5.04-21.el6
file-devel-5.04-21.el6
file-static-5.04-21.el6
file-debuginfo-5.04-21.el6
python-magic-5.04-21.el6
file-libs-5.04-21.el6

i386
file-5.04-21.el6
file-devel-5.04-21.el6
file-static-5.04-21.el6
file-debuginfo-5.04-21.el6
python-magic-5.04-21.el6
file-libs-5.04-21.el6

174583 - Scientific Linux Security ERRATA Moderate: cups on SL6.x i386/x86_64 (1411-1231)

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

Risk Level: Medium

CVE: CVE-2014-2856, CVE-2014-3537, CVE-2014-5029, CVE-2014-5030, CVE-2014-5031

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: cups on SL6.x i386/x86_64 (1411-1231)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1231

SL6
x86_64
cups-devel-1.4.2-67.el6
cups-libs-1.4.2-67.el6
cups-php-1.4.2-67.el6
cups-lpd-1.4.2-67.el6
cups-debuginfo-1.4.2-67.el6
cups-1.4.2-67.el6

i386
cups-devel-1.4.2-67.el6
cups-libs-1.4.2-67.el6
cups-php-1.4.2-67.el6
cups-lpd-1.4.2-67.el6
cups-debuginfo-1.4.2-67.el6
cups-1.4.2-67.el6

85819 - CentOS 7 CESA-2014-1795 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4337, CVE-2014-4338

Description

The scan detected that the host is missing the following update:
CESA-2014-1795

Observation

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

http://lists.centos.org/pipermail/centos-announce/2014-November/020734.html

CentOS 7
i686
cups-filters-devel-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-devel-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

91652 - Oracle Enterprise Linux ELSA-2014-1795 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4337, CVE-2014-4338

Description

The scan detected that the host is missing the following update:
ELSA-2014-1795

Observation

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

http://oss.oracle.com/pipermail/el-errata/2014-November/004606.html

OEL7
x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-devel-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

140602 - Red Hat Enterprise Linux RHSA-2014-1795 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4337, CVE-2014-4338

Description

The scan detected that the host is missing the following update:
RHSA-2014-1795

Observation

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

https://rhn.redhat.com/errata/RHSA-2014-1795.html

RHEL7WS
x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-debuginfo-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

RHEL7D
x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-debuginfo-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

RHEL7S
x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-debuginfo-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

174574 - Scientific Linux Security ERRATA Moderate: cups-filters on SL7.x x86_64 (1411-1865)

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

Risk Level: Medium

CVE: CVE-2014-4337, CVE-2014-4338

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: cups-filters on SL7.x x86_64 (1411-1865)

Observation

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

http://listserv.fnal.gov/scripts/wa.exe?A2=ind1411&L=scientific-linux-errata&T=0&P=1865

SL7
x86_64
cups-filters-1.0.35-15.el7_0.1
cups-filters-devel-1.0.35-15.el7_0.1
cups-filters-debuginfo-1.0.35-15.el7_0.1
cups-filters-libs-1.0.35-15.el7_0.1

58985 - Debian Linux 7.0 DSA-3063-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8483

Description

The scan detected that the host is missing the following update:
DSA-3063-1

Observation

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

http://www.debian.org/security/2014/dsa-3063

Debian 7.0
all
quassel_0.8.0-1+deb7u3

58986 - Debian Linux 7.0 DSA-3060-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3610, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-3647, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-7207

Description

The scan detected that the host is missing the following update:
DSA-3060-1

Observation

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

http://www.debian.org/security/2014/dsa-3060

Debian 7.0
all
pata-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
nbd-modules-3.2.0-4-versatile-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-versatile-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-loongson-2f-di_3.2.63-2+deb7u1
core-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
loop-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
linux-image-3.2.0-4-s390x_3.2.63-2+deb7u1
kernel-image-3.2.0-4-486-di_3.2.63-2+deb7u1
ext4-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-powerpc64_3.2.63-2+deb7u1
sata-modules-3.2.0-4-loongson-2f-di_3.2.63-2+deb7u1
nic-shared-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
ipv6-modules-3.2.0-4-r4k-ip22-di_3.2.63-2+deb7u1
linux-image-3.2.0-4-versatile_3.2.63-2+deb7u1
ppp-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
nbd-modules-3.2.0-4-iop32x-di_3.2.63-2+deb7u1
nic-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
crypto-dm-modules-3.2.0-4-loongson-2f-di_3.2.63-2+deb7u1
floppy-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
md-modules-3.2.0-4-r5k-cobalt-di_3.2.63-2+deb7u1
nic-shared-modules-3.2.0-4-mx5-di_3.2.63-2+deb7u1
ipv6-modules-3.2.0-4-mx5-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-vexpress_3.2.63-2+deb7u1
linux-image-3.2.0-4-kirkwood_3.2.63-2+deb7u1
multipath-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
usb-serial-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
linux-image-3.2.0-4-rt-686-pae-dbg_3.2.63-2+deb7u1
plip-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
zlib-modules-3.2.0-4-r5k-ip32-di_3.2.63-2+deb7u1
reiserfs-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
ext4-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
irda-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
squashfs-modules-3.2.0-4-r4k-ip22-di_3.2.63-2+deb7u1
xfs-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
pcmcia-storage-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
ppp-modules-3.2.0-4-iop32x-di_3.2.63-2+deb7u1
uinput-modules-3.2.0-4-kirkwood-di_3.2.63-2+deb7u1
scsi-core-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
crypto-dm-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
zlib-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
zlib-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
scsi-core-modules-3.2.0-4-sb1-bcm91250a-di_3.2.63-2+deb7u1
squashfs-modules-3.2.0-4-r5k-cobalt-di_3.2.63-2+deb7u1
nic-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
btrfs-modules-3.2.0-4-mx5-di_3.2.63-2+deb7u1
multipath-modules-3.2.0-4-sb1-bcm91250a-di_3.2.63-2+deb7u1
btrfs-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
xfs-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
mouse-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
ufs-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
loop-modules-3.2.0-4-r5k-ip32-di_3.2.63-2+deb7u1
sata-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
crypto-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
kernel-image-3.2.0-4-sparc64-di_3.2.63-2+deb7u1

linux-headers-3.2.0-4-octeon_3.2.63-2+deb7u1
nic-wireless-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
ext4-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
jfs-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
xfs-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
fat-modules-3.2.0-4-mx5-di_3.2.63-2+deb7u1
reiserfs-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
xfs-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
input-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
speakup-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
md-modules-3.2.0-4-sb1-bcm91250a-di_3.2.63-2+deb7u1
plip-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
usb-serial-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
mmc-core-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
event-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-s390x_3.2.63-2+deb7u1
kernel-image-3.2.0-4-itanium-di_3.2.63-2+deb7u1
crypto-dm-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
nic-wireless-modules-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
sata-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
nic-usb-modules-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
loop-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-kirkwood-di_3.2.63-2+deb7u1
plip-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
linux-libc-dev_3.2.63-2+deb7u1
scsi-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
btrfs-modules-3.2.0-4-loongson-2f-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
kernel-image-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
udf-modules-3.2.0-4-sparc64-di_3.2.63-2+deb7u1
pcmcia-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
ipv6-modules-3.2.0-4-iop32x-di_3.2.63-2+deb7u1
ext3-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
multipath-modules-3.2.0-4-mx5-di_3.2.63-2+deb7u1
udf-modules-3.2.0-4-iop32x-di_3.2.63-2+deb7u1
isofs-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
i2c-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
nic-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
squashfs-modules-3.2.0-4-sb1-bcm91250a-di_3.2.63-2+deb7u1
nic-wireless-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
linux-image-3.2.0-4-sparc64-smp_3.2.63-2+deb7u1
kernel-image-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
usb-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
md-modules-3.2.0-4-r4k-ip22-di_3.2.63-2+deb7u1
event-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
fancontrol-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
crypto-dm-modules-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
usb-storage-modules-3.2.0-4-loongson-2f-di_3.2.63-2+deb7u1
usb-storage-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
scsi-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
irda-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
firewire-core-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
jfs-modules-3.2.0-4-kirkwood-di_3.2.63-2+deb7u1
crypto-modules-3.2.0-4-amd64-di_3.2.63-2+deb7u1
virtio-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
udf-modules-3.2.0-4-itanium-di_3.2.63-2+deb7u1
btrfs-modules-3.2.0-4-r4k-ip22-di_3.2.63-2+deb7u1
udf-modules-3.2.0-4-versatile-di_3.2.63-2+deb7u1

scsi-core-modules-3.2.0-4-versatile-di_3.2.63-2+deb7u1
md-modules-3.2.0-4-r5k-ip32-di_3.2.63-2+deb7u1
linux-support-3.2.0-4_3.2.63-2+deb7u1
squashfs-modules-3.2.0-4-vexpress-di_3.2.63-2+deb7u1
scsi-core-modules-3.2.0-4-powerpc64-di_3.2.63-2+deb7u1
ext4-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-common_3.2.63-2+deb7u1
nic-shared-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
ipv6-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-orion5x_3.2.63-2+deb7u1
nbd-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1
nic-pcmcia-modules-3.2.0-4-powerpc-di_3.2.63-2+deb7u1
dasd-extra-modules-3.2.0-4-s390x-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-all-sparc_3.2.63-2+deb7u1
kernel-image-3.2.0-4-sb1-bcm91250a-di_3.2.63-2+deb7u1
nic-modules-3.2.0-4-s390x-di_3.2.63-2+deb7u1
ext2-modules-3.2.0-4-orion5x-di_3.2.63-2+deb7u1
fat-modules-3.2.0-4-486-di_3.2.63-2+deb7u1
dasd-modules-3.2.0-4-s390x-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-mx5_3.2.63-2+deb7u1
kernel-image-3.2.0-4-r4k-ip22-di_3.2.63-2+deb7u1
udf-modules-3.2.0-4-kirkwood-di_3.2.63-2+deb7u1
linux-headers-3.2.0-4-rt-amd64_3.2.63-2+deb7u1
scsi-modules-3.2.0-4-686-pae-di_3.2.63-2+deb7u1
sata-modules-3.2.0-4-4kc-malta-di_3.2.63-2+deb7u1

88646 - Slackware Linux 14.0, 14.1 SSA:2014-307-04 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:2014-307-04

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=2014&m=slackware-security.490480

Slackware 14.0
x86_64
seamonkey-2.30-x86_64-1
seamonkey-solibs-2.30-x86_64-1

Slackware 14.1
x86_64
seamonkey-2.30-x86_64-1
seamonkey-solibs-2.30-x86_64-1

88647 - Slackware Linux 14.1 SSA:2014-307-02 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:2014-307-02

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=2014&m=slackware-security.356277

Slackware 14.1
x86_64
mozilla-firefox-31.2.0esr-x86_64-1

142476 - SuSE Linux 13.1 openSUSE-SU-2014:1348-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-7300

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1348-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-11/msg00005.html

SuSE Linux 13.1
i586
gnome-settings-daemon-debuginfo-3.10.3-24.1
gnome-settings-daemon-3.10.3-24.1
gnome-settings-daemon-lang-3.10.3-24.1
gnome-settings-daemon-debugsource-3.10.3-24.1
gnome-settings-daemon-devel-3.10.3-24.1

142477 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1330-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3660

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2014:1330-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2014-10/msg00034.html

SuSE Linux 13.1
i586
libxml2-devel-2.9.1-2.16.1
libxml2-tools-debuginfo-2.9.1-2.16.1
libxml2-2-debuginfo-2.9.1-2.16.1
python-libxml2-debugsource-2.9.1-2.16.1
libxml2-debugsource-2.9.1-2.16.1
python-libxml2-debuginfo-2.9.1-2.16.1
libxml2-2-2.9.1-2.16.1
python-libxml2-2.9.1-2.16.1
libxml2-tools-2.9.1-2.16.1

x86_64
libxml2-devel-32bit-2.9.1-2.16.1
libxml2-2-debuginfo-32bit-2.9.1-2.16.1
libxml2-2-32bit-2.9.1-2.16.1
libxml2-doc-2.9.1-2.16.1

SuSE Linux 12.3
i586
python-libxml2-2.9.0-2.33.1
libxml2-2-2.9.0-2.33.1
python-libxml2-debugsource-2.9.0-2.33.1
libxml2-debugsource-2.9.0-2.33.1
libxml2-tools-2.9.0-2.33.1
libxml2-2-debuginfo-2.9.0-2.33.1
libxml2-devel-2.9.0-2.33.1
python-libxml2-debuginfo-2.9.0-2.33.1
libxml2-tools-debuginfo-2.9.0-2.33.1

x86_64
libxml2-devel-32bit-2.9.0-2.33.1
libxml2-2-debuginfo-32bit-2.9.0-2.33.1
libxml2-doc-2.9.0-2.33.1
libxml2-2-32bit-2.9.0-2.33.1

181282 - FreeBSD twiki Remote Perl Code Execution (21ce1840-6107-11e4-9e84-0022156e8794)

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

Risk Level: Low

CVE: CVE-2014-7236

Description

The scan detected that the host is missing the following update:
twiki -- remote Perl code execution (21ce1840-6107-11e4-9e84-0022156e8794)

Observation

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

http://www.vuxml.org/freebsd/21ce1840-6107-11e4-9e84-0022156e8794.html

Affected packages:
twiki < 5.1.4_1,1

181283 - FreeBSD jenkins Slave-originated Arbitrary Code Execution On Master Servers (0dad9114-60cc-11e4-9e84-0022156e8794)

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

Risk Level: Low

CVE: CVE-2014-3665

Description

The scan detected that the host is missing the following update:
jenkins -- slave-originated arbitrary code execution on master servers (0dad9114-60cc-11e4-9e84-0022156e8794)

Observation

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

http://www.vuxml.org/freebsd/0dad9114-60cc-11e4-9e84-0022156e8794.html

Affected packages:
jenkins < 1.587
jenkins-lts < 1.580.1

43148 - HP-UX 11.X PHCO_44198 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
PHCO_44198

Observation

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

https://www11.itrc.hp.com/service/patch/patchDetail.do?patchid=PHCO_44198

">patch description

HP-UX 11.31 (NA)

VRTSvxfs.VXFS-RUN,fr=5.0.31.0,fa=HP-UX_B.11.31_PA,v=Symantec
VRTSvxfs.VXFS-RUN-PALIB,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=Symantec
VRTSvxfs.VXFS-PRG,fr=5.0.31.0,fa=HP-UX_B.11.31_PA,v=Symantec
VRTSvxfs.VXFS-RUN,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=Symantec
VRTSvxfs.VXFS-PRG,fr=5.0.31.0,fa=HP-UX_B.11.31_PA,v=HP
VRTSvxfs.VXFS-PRG,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=Symantec
VRTSvxfs.VXFS-PRG,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=HP
VRTSvxfs.VXFS-RUN,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=HP
VRTSvxfs.VXFS-RUN-PALIB,fr=5.0.31.0,fa=HP-UX_B.11.31_IA,v=HP
VRTSvxfs.VXFS-RUN,fr=5.0.31.0,fa=HP-UX_B.11.31_PA,v=HP

181281 - FreeBSD libssh PRNG State Reuse On Forking Servers (f8c88d50-5fb3-11e4-81bd-5453ed2e2b49)

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

Risk Level: Low

CVE: CVE-2014-0017

Description

The scan detected that the host is missing the following update:
libssh -- PRNG state reuse on forking servers (f8c88d50-5fb3-11e4-81bd-5453ed2e2b49)

Observation

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

http://www.vuxml.org/freebsd/f8c88d50-5fb3-11e4-81bd-5453ed2e2b49.html

Affected packages:
libssh < 0.6.3

ENHANCED CHECKS

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

15409 - McAfee Data Loss Prevention Multiple Vulnerabilities Prior To 9.3

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-1999-0524, CVE-2000-0219, CVE-2004-0230, CVE-2014-8520, CVE-2014-8521, CVE-2014-8522, CVE-2014-8523, CVE-2014-8524, CVE-2014-8525, CVE-2014-8526, CVE-2014-8527, CVE-2014-8528, CVE-2014-8529, CVE-2014-8530, CVE-2014-8531, CVE-2014-8532, CVE-2014-8533

Update Details

CVE is updated

16808 - (SB10075) McAfee ePolicy Orchestrator OpenSSL Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-0195, CVE-2010-5298, CVE-2014-0076, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Update Details

FASLScript is updated

17039 - BlackBerry OS OpenSSL Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

Update Details

Recommendation is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Update Details

Recommendation is updated

15322 - McAfee Data Loss Prevention Manager Multiple Vulnerabilities Prior To 9.2.2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2014-8519, CVE-2014-8534, CVE-2014-8535, CVE-2014-8536, CVE-2014-8537

Update Details

CVE is updated

33116 - Oracle Solaris 150383-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33277 - Oracle Solaris 150512-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Update Details

CVE is updated

33278 - Oracle Solaris 150513-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Update Details

CVE is updated

142466 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 perl-9858 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-4330

Update Details

FASLScript is updated

DELETED CHECKS

723 - Solaris AnswerBook2 Unauthorized Admin Access

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

Risk Level: High

CVE: CVE-2000-0696

779 - OReilly WebSitePro uploader.exe File Upload

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

Risk Level: High

CVE: CVE-2000-0769

7890 - TLS / SSL Man-In-The-Middle Renegotiation Vulnerability

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3555

43120 - HP-UX 11.X PHCO_43685 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

43127 - HP-UX 11.X PHKL_43513 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

ADDITIONAL NOTES

- **723** - has been replaced by FID 17335.
- **779** - has been identified as obsolete.
- **43120** - was flagged as obsolete by the vendor.
- **43127** - was flagged as obsolete by the vendor.
- **7890** - has been replaced by FID 9763.

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.