2015-NOV-11
FSL version 7.5.761

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

144028 - SuSE Linux 13.2 openSUSE-SU-2015:1905-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1905-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00031.html

SuSE Linux 13.2
i586
java-1_8_0-openjdk-headless-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-src-1.8.0.65-18.1
java-1_8_0-openjdk-demo-1.8.0.65-18.1
java-1_8_0-openjdk-headless-1.8.0.65-18.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-accessibility-1.8.0.65-18.1
java-1_8_0-openjdk-1.8.0.65-18.1
java-1_8_0-openjdk-devel-1.8.0.65-18.1
java-1_8_0-openjdk-debugsource-1.8.0.65-18.1

noarch
java-1_8_0-openjdk-javadoc-1.8.0.65-18.1

x86_64
java-1_8_0-openjdk-headless-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-src-1.8.0.65-18.1
java-1_8_0-openjdk-demo-1.8.0.65-18.1
java-1_8_0-openjdk-headless-1.8.0.65-18.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-debuginfo-1.8.0.65-18.1
java-1_8_0-openjdk-accessibility-1.8.0.65-18.1
java-1_8_0-openjdk-1.8.0.65-18.1
java-1_8_0-openjdk-devel-1.8.0.65-18.1
java-1_8_0-openjdk-debugsource-1.8.0.65-18.1

144032 - SuSE Linux 13.1 openSUSE-SU-2015:1906-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1906-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00032.html

SuSE Linux 13.1
i586
java-1_7_0-openjdk-debugsource-1.7.0.91-24.24.1
java-1_7_0-openjdk-src-1.7.0.91-24.24.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-accessibility-1.7.0.91-24.24.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-devel-1.7.0.91-24.24.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-headless-1.7.0.91-24.24.1
java-1_7_0-openjdk-1.7.0.91-24.24.1
java-1_7_0-openjdk-demo-1.7.0.91-24.24.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.91-24.24.1

x86_64
java-1_7_0-openjdk-debugsource-1.7.0.91-24.24.1
java-1_7_0-openjdk-src-1.7.0.91-24.24.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-accessibility-1.7.0.91-24.24.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-devel-1.7.0.91-24.24.1
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-debuginfo-1.7.0.91-24.24.1
java-1_7_0-openjdk-headless-1.7.0.91-24.24.1
java-1_7_0-openjdk-1.7.0.91-24.24.1
java-1_7_0-openjdk-demo-1.7.0.91-24.24.1

144045 - SuSE Linux 13.2 openSUSE-SU-2015:1902-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1902-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00028.html

SuSE Linux 13.2
i586
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-demo-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-debugsource-1.7.0.91-13.1
java-1_7_0-openjdk-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.91-13.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-src-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-1.7.0.91-13.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-headless-1.7.0.91-13.1
java-1_7_0-openjdk-accessibility-1.7.0.91-13.1
java-1_7_0-openjdk-devel-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.91-13.1

noarch
java-1_7_0-openjdk-javadoc-1.7.0.91-13.1

x86_64
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-demo-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-headless-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-debugsource-1.7.0.91-13.1
java-1_7_0-openjdk-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-devel-1.7.0.91-13.1
java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-src-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-1.7.0.91-13.1
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-13.1
java-1_7_0-openjdk-headless-1.7.0.91-13.1
java-1_7_0-openjdk-accessibility-1.7.0.91-13.1
java-1_7_0-openjdk-devel-1.7.0.91-13.1
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.91-13.1

88719 - Slackware Linux 14.0, 14.1 SSA:2015-310-02 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SSA:2015-310-02

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.399753

Slackware 14.1
x86_64
mozilla-nss-3.20.1-x86_64-1

Slackware 14.0
x86_64
mozilla-nss-3.20.1-x86_64-1

91927 - Oracle Enterprise Linux ELSA-2015-1980 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2015-1980

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005492.html

OEL5
i386
nss-3.19.1-2.el5_11
nss-tools-3.19.1-2.el5_11
nspr-devel-4.10.8-2.el5_11
nspr-4.10.8-2.el5_11
nss-devel-3.19.1-2.el5_11
nss-pkcs11-devel-3.19.1-2.el5_11

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

91928 - Oracle Enterprise Linux ELSA-2015-1981 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2015-1981

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005490.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005494.html

OEL7
x86_64
nss-tools-3.19.1-7.0.1.el7_1.2
nspr-4.10.8-2.el7_1
nss-sysinit-3.19.1-7.0.1.el7_1.2
nss-devel-3.19.1-7.0.1.el7_1.2
nss-3.19.1-7.0.1.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-util-3.19.1-4.el7_1
nss-pkcs11-devel-3.19.1-7.0.1.el7_1.2
nss-util-devel-3.19.1-4.el7_1

OEL6
x86_64
nss-tools-3.19.1-5.0.1.el6_7
nss-devel-3.19.1-5.0.1.el6_7
nss-3.19.1-5.0.1.el6_7
nspr-4.10.8-2.el6_7
nss-sysinit-3.19.1-5.0.1.el6_7
nss-util-3.19.1-2.el6_7
nspr-devel-4.10.8-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.0.1.el6_7

i386
nss-tools-3.19.1-5.0.1.el6_7
nss-devel-3.19.1-5.0.1.el6_7
nss-3.19.1-5.0.1.el6_7
nspr-4.10.8-2.el6_7
nss-sysinit-3.19.1-5.0.1.el6_7
nss-util-3.19.1-2.el6_7
nspr-devel-4.10.8-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.0.1.el6_7

91929 - Oracle Enterprise Linux ELSA-2015-1982 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ELSA-2015-1982

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005495.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005493.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005491.html

OEL5
x86_64
firefox-38.4.0-1.0.1.el5_11

i386
firefox-38.4.0-1.0.1.el5_11

OEL6
x86_64
firefox-38.4.0-1.0.1.el6_7

i386
firefox-38.4.0-1.0.1.el6_7

OEL7
x86_64
firefox-38.4.0-1.0.1.el7_1

96020 - CentOS 6, 7 CESA-2015-1981 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2015-1981

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021464.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021466.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021465.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021470.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021468.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021469.html

CentOS 7
x86_64
nspr-4.10.8-2.el7_1
nss-devel-3.19.1-7.el7_1.2
nss-pkcs11-devel-3.19.1-7.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-3.19.1-7.el7_1.2

nss-tools-3.19.1-7.el7_1.2
nss-sysinit-3.19.1-7.el7_1.2
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

i686
nspr-4.10.8-2.el7_1
nss-devel-3.19.1-7.el7_1.2
nss-pkcs11-devel-3.19.1-7.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-3.19.1-7.el7_1.2
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

CentOS 6
x86_64
nss-util-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-tools-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nspr-devel-4.10.8-2.el6_7

i686
nss-util-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-tools-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nspr-devel-4.10.8-2.el6_7

96022 - CentOS 5 CESA-2015-1980 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
CESA-2015-1980

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021473.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021472.html

CentOS 5
x86_64
nss-3.19.1-2.el5_11
nss-tools-3.19.1-2.el5_11

nspr-devel-4.10.8-2.el5_11
nspr-4.10.8-2.el5_11
nss-devel-3.19.1-2.el5_11
nss-pkcs11-devel-3.19.1-2.el5_11

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

96023 - CentOS 5, 6, 7 CESA-2015-1982 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
CESA-2015-1982

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021474.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021467.html
http://lists.centos.org/pipermail/centos-announce/2015-November/021471.html

CentOS 6
x86_64
firefox-38.4.0-1.el6.centos

i686
firefox-38.4.0-1.el6.centos

CentOS 7
x86_64
firefox-38.4.0-1.el7.centos

i686
firefox-38.4.0-1.el7.centos

CentOS 5
x86_64
firefox-38.4.0-1.el5.centos

i386
firefox-38.4.0-1.el5.centos

130312 - Debian Linux 7.0, 8.0 DSA-3395-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2695, CVE-2015-2696, CVE-2015-2697

Description

The scan detected that the host is missing the following update:
DSA-3395-1

Observation

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

http://www.debian.org/security/2015/dsa-3395

Debian 8.0
all
libkrad-dev_1.12.1+dfsg-19+deb8u1
libkrb5support0_1.12.1+dfsg-19+deb8u1
krb5-user_1.12.1+dfsg-19+deb8u1
libgssapi-krb5-2_1.12.1+dfsg-19+deb8u1
libkrb5-dev_1.12.1+dfsg-19+deb8u1
krb5-doc_1.12.1+dfsg-19+deb8u1
krb5-pkinit_1.12.1+dfsg-19+deb8u1
libkadm5srv-mit9_1.12.1+dfsg-19+deb8u1
libkrad0_1.12.1+dfsg-19+deb8u1
libkrb5-dbg_1.12.1+dfsg-19+deb8u1
libkdb5-7_1.12.1+dfsg-19+deb8u1
libkrb5-3_1.12.1+dfsg-19+deb8u1
krb5-multidev_1.12.1+dfsg-19+deb8u1
libgssrpc4_1.12.1+dfsg-19+deb8u1
krb5-kdc_1.12.1+dfsg-19+deb8u1
krb5-otp_1.12.1+dfsg-19+deb8u1
krb5-admin-server_1.12.1+dfsg-19+deb8u1
krb5-kdc-ldap_1.12.1+dfsg-19+deb8u1
libk5crypto3_1.12.1+dfsg-19+deb8u1
krb5-locales_1.12.1+dfsg-19+deb8u1
libkadm5clnt-mit9_1.12.1+dfsg-19+deb8u1
krb5-gss-samples_1.12.1+dfsg-19+deb8u1

Debian 7.0
all
libkrb5support0_1.10.1+dfsg-5+deb7u4
libkrb5-3_1.10.1+dfsg-5+deb7u4
libk5crypto3_1.10.1+dfsg-5+deb7u4
krb5-user_1.10.1+dfsg-5+deb7u4
krb5-kdc_1.10.1+dfsg-5+deb7u4
libgssrpc4_1.10.1+dfsg-5+deb7u4
libkrb5-dev_1.10.1+dfsg-5+deb7u4
krb5-locales_1.10.1+dfsg-5+deb7u4
libkrb5-dbg_1.10.1+dfsg-5+deb7u4
libgssapi-krb5-2_1.10.1+dfsg-5+deb7u4
krb5-admin-server_1.10.1+dfsg-5+deb7u4
krb5-doc_1.10.1+dfsg-5+deb7u4
krb5-multidev_1.10.1+dfsg-5+deb7u4
libkadm5srv-mit8_1.10.1+dfsg-5+deb7u4
krb5-kdc-ldap_1.10.1+dfsg-5+deb7u4
krb5-gss-samples_1.10.1+dfsg-5+deb7u4
libkadm5clnt-mit8_1.10.1+dfsg-5+deb7u4
libkdb5-6_1.10.1+dfsg-5+deb7u4
krb5-pkinit_1.10.1+dfsg-5+deb7u4

130314 - Debian Linux 7.0, 8.0 DSA-3393-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
DSA-3393-1

Observation

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

http://www.debian.org/security/2015/dsa-3393

Debian 8.0
all
iceweasel_38.4.0esr-1~deb8u1

Debian 7.0
all
iceweasel_38.4.0esr-1~deb7u1

132197 - Oracle VM OVMSA-2015-0145 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0145

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-November/000376.html

OVM3.3
x86_64
nss-util-3.19.1-2.el6_7
nss-tools-3.19.1-5.0.1.el6_7
nss-sysinit-3.19.1-5.0.1.el6_7
nspr-4.10.8-2.el6_7
nss-3.19.1-5.0.1.el6_7

132198 - Oracle VM OVMSA-2015-0143 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7835, CVE-2015-7969, CVE-2015-7971

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0143

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-November/000393.html

OVM3.2
x86_64
xen-4.1.3-25.el5.209.4
xen-devel-4.1.3-25.el5.209.4
xen-tools-4.1.3-25.el5.209.4

140969 - Red Hat Enterprise Linux RHSA-2015-1980 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2015-1980

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-1980.html

RHEL5D
x86_64
nspr-4.10.8-2.el5_11
nss-tools-3.19.1-2.el5_11
nspr-devel-4.10.8-2.el5_11
nss-devel-3.19.1-2.el5_11
nspr-debuginfo-4.10.8-2.el5_11
nss-pkcs11-devel-3.19.1-2.el5_11
nss-3.19.1-2.el5_11
nss-debuginfo-3.19.1-2.el5_11

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

RHEL5S
i386
nspr-4.10.8-2.el5_11
nss-tools-3.19.1-2.el5_11

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

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

140970 - Red Hat Enterprise Linux RHSA-2015-1982 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
RHSA-2015-1982

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-1982.html

RHEL5S
i386
firefox-debuginfo-38.4.0-1.el5_11
firefox-38.4.0-1.el5_11

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

RHEL7S
x86_64
firefox-debuginfo-38.4.0-1.el7_1
firefox-38.4.0-1.el7_1

RHEL6S
i386
firefox-38.4.0-1.el6_7
firefox-debuginfo-38.4.0-1.el6_7

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

RHEL6WS

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

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

RHEL5D
x86_64
firefox-debuginfo-38.4.0-1.el5_11
firefox-38.4.0-1.el5_11

i386
firefox-debuginfo-38.4.0-1.el5_11
firefox-38.4.0-1.el5_11

RHEL7D
x86_64
firefox-debuginfo-38.4.0-1.el7_1
firefox-38.4.0-1.el7_1

RHEL6D
x86_64
firefox-38.4.0-1.el6_7
firefox-debuginfo-38.4.0-1.el6_7

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

RHEL7WS
x86_64
firefox-debuginfo-38.4.0-1.el7_1
firefox-38.4.0-1.el7_1

140972 - Red Hat Enterprise Linux RHSA-2015-1981 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2015-1981

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-1981.html

RHEL7S
x86_64
nss-util-debuginfo-3.19.1-4.el7_1
nspr-4.10.8-2.el7_1
nspr-debuginfo-4.10.8-2.el7_1
nss-tools-3.19.1-7.el7_1.2

nss-pkcs11-devel-3.19.1-7.el7_1.2
nss-devel-3.19.1-7.el7_1.2
nss-3.19.1-7.el7_1.2
nss-debuginfo-3.19.1-7.el7_1.2
nss-sysinit-3.19.1-7.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

RHEL6S
i386
nss-util-3.19.1-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7

x86_64
nss-util-3.19.1-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7

RHEL6WS
x86_64
nss-util-3.19.1-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

i386
nss-util-3.19.1-2.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7

nss-sysinit-3.19.1-5.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

RHEL7D
x86_64
nss-util-debuginfo-3.19.1-4.el7_1
nspr-4.10.8-2.el7_1
nspr-debuginfo-4.10.8-2.el7_1
nss-tools-3.19.1-7.el7_1.2
nss-pkcs11-devel-3.19.1-7.el7_1.2
nspr-devel-4.10.8-2.el7_1
nss-devel-3.19.1-7.el7_1.2
nss-3.19.1-7.el7_1.2
nss-debuginfo-3.19.1-7.el7_1.2
nss-sysinit-3.19.1-7.el7_1.2
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

RHEL6D
x86_64
nss-util-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

i386
nss-util-3.19.1-2.el6_7
nss-pkcs11-devel-3.19.1-5.el6_7
nss-3.19.1-5.el6_7
nspr-4.10.8-2.el6_7
nss-util-debuginfo-3.19.1-2.el6_7
nss-tools-3.19.1-5.el6_7
nss-debuginfo-3.19.1-5.el6_7
nss-sysinit-3.19.1-5.el6_7
nss-util-devel-3.19.1-2.el6_7
nss-devel-3.19.1-5.el6_7
nspr-devel-4.10.8-2.el6_7
nspr-debuginfo-4.10.8-2.el6_7

RHEL7WS
x86_64
nss-util-debuginfo-3.19.1-4.el7_1
nspr-4.10.8-2.el7_1
nspr-debuginfo-4.10.8-2.el7_1
nss-tools-3.19.1-7.el7_1.2
nss-pkcs11-devel-3.19.1-7.el7_1.2
nss-devel-3.19.1-7.el7_1.2
nss-3.19.1-7.el7_1.2
nss-debuginfo-3.19.1-7.el7_1.2
nss-sysinit-3.19.1-7.el7_1.2

nspr-devel-4.10.8-2.el7_1
nss-util-3.19.1-4.el7_1
nss-util-devel-3.19.1-4.el7_1

144027 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1926-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1926-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001671.html

SuSE SLED 12
x86_64
libsoftokn3-32bit-3.19.2.1-29.1
libfreebl3-debuginfo-32bit-3.19.2.1-29.1
libsoftokn3-3.19.2.1-29.1
mozilla-nss-32bit-3.19.2.1-29.1
libfreebl3-3.19.2.1-29.1
mozilla-nss-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-38.4.0esr-51.1
MozillaFirefox-branding-SLE-31.0-17.1
libfreebl3-32bit-3.19.2.1-29.1
mozilla-nspr-debuginfo-32bit-4.10.10-9.1
mozilla-nss-certs-3.19.2.1-29.1
mozilla-nss-certs-32bit-3.19.2.1-29.1
libsoftokn3-debuginfo-3.19.2.1-29.1
mozilla-nss-debugsource-3.19.2.1-29.1
mozilla-nspr-debugsource-4.10.10-9.1
mozilla-nss-debuginfo-3.19.2.1-29.1
libsoftokn3-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-translations-38.4.0esr-51.1
mozilla-nspr-4.10.10-9.1
mozilla-nss-certs-debuginfo-3.19.2.1-29.1
MozillaFirefox-debuginfo-38.4.0esr-51.1
libfreebl3-debuginfo-3.19.2.1-29.1
mozilla-nss-tools-3.19.2.1-29.1
mozilla-nss-tools-debuginfo-3.19.2.1-29.1
mozilla-nspr-debuginfo-4.10.10-9.1
mozilla-nss-3.19.2.1-29.1
mozilla-nss-certs-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-debugsource-38.4.0esr-51.1
mozilla-nspr-32bit-4.10.10-9.1

SuSE SLES 12
x86_64
libsoftokn3-32bit-3.19.2.1-29.1
libfreebl3-debuginfo-32bit-3.19.2.1-29.1
libsoftokn3-3.19.2.1-29.1

libfreebl3-hmac-32bit-3.19.2.1-29.1
mozilla-nss-32bit-3.19.2.1-29.1
libfreebl3-3.19.2.1-29.1
mozilla-nss-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-38.4.0esr-51.1
MozillaFirefox-branding-SLE-31.0-17.1
libsoftokn3-hmac-32bit-3.19.2.1-29.1
libfreebl3-32bit-3.19.2.1-29.1
mozilla-nspr-debuginfo-32bit-4.10.10-9.1
mozilla-nss-certs-3.19.2.1-29.1
libsoftokn3-hmac-3.19.2.1-29.1
mozilla-nss-certs-32bit-3.19.2.1-29.1
libsoftokn3-debuginfo-3.19.2.1-29.1
mozilla-nss-debugsource-3.19.2.1-29.1
mozilla-nspr-debugsource-4.10.10-9.1
mozilla-nss-debuginfo-3.19.2.1-29.1
libsoftokn3-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-translations-38.4.0esr-51.1
mozilla-nspr-4.10.10-9.1
mozilla-nss-certs-debuginfo-3.19.2.1-29.1
MozillaFirefox-debuginfo-38.4.0esr-51.1
libfreebl3-debuginfo-3.19.2.1-29.1
mozilla-nss-tools-3.19.2.1-29.1
mozilla-nss-tools-debuginfo-3.19.2.1-29.1
mozilla-nspr-debuginfo-4.10.10-9.1
libfreebl3-hmac-3.19.2.1-29.1
mozilla-nss-3.19.2.1-29.1
mozilla-nss-certs-debuginfo-32bit-3.19.2.1-29.1
MozillaFirefox-debugsource-38.4.0esr-51.1
mozilla-nspr-32bit-4.10.10-9.1

144029 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1904-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1904-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00030.html

SuSE Linux 13.1
noarch
roundcubemail-1.0.7-2.24.1

SuSE Linux 13.2
noarch
roundcubemail-1.0.7-14.1

144031 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1908-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0222, CVE-2015-4037, CVE-2015-5239, CVE-2015-6815, CVE-2015-7311, CVE-2015-7835, CVE-2015-7969, CVE-2015-7971

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1908-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001668.html

SuSE SLED 12
x86_64
xen-libs-debuginfo-32bit-4.4.3_02-22.12.1
xen-debugsource-4.4.3_02-22.12.1
xen-libs-4.4.3_02-22.12.1
xen-kmp-default-4.4.3_02_k3.12.48_52.27-22.12.1
xen-4.4.3_02-22.12.1
xen-libs-32bit-4.4.3_02-22.12.1
xen-libs-debuginfo-4.4.3_02-22.12.1
xen-kmp-default-debuginfo-4.4.3_02_k3.12.48_52.27-22.12.1

SuSE SLES 12
x86_64
xen-tools-debuginfo-4.4.3_02-22.12.1
xen-libs-32bit-4.4.3_02-22.12.1
xen-tools-domU-debuginfo-4.4.3_02-22.12.1
xen-tools-domU-4.4.3_02-22.12.1
xen-kmp-default-debuginfo-4.4.3_02_k3.12.48_52.27-22.12.1
xen-tools-4.4.3_02-22.12.1
xen-kmp-default-4.4.3_02_k3.12.48_52.27-22.12.1
xen-4.4.3_02-22.12.1
xen-libs-debuginfo-4.4.3_02-22.12.1
xen-debugsource-4.4.3_02-22.12.1
xen-libs-4.4.3_02-22.12.1
xen-libs-debuginfo-32bit-4.4.3_02-22.12.1
xen-doc-html-4.4.3_02-22.12.1

144034 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1928-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2695, CVE-2015-2696, CVE-2015-2697

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1928-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00043.html

SuSE Linux 13.1
x86_64
krb5-debuginfo-32bit-1.11.3-3.21.1
krb5-mini-debuginfo-1.11.3-3.21.1
krb5-debuginfo-1.11.3-3.21.1
krb5-doc-1.11.3-3.21.1
krb5-plugin-preauth-pkinit-1.11.3-3.21.1
krb5-1.11.3-3.21.1
krb5-plugin-preauth-pkinit-debuginfo-1.11.3-3.21.1
krb5-plugin-kdb-ldap-debuginfo-1.11.3-3.21.1
krb5-plugin-kdb-ldap-1.11.3-3.21.1
krb5-client-debuginfo-1.11.3-3.21.1
krb5-mini-devel-1.11.3-3.21.1
krb5-mini-1.11.3-3.21.1
krb5-server-1.11.3-3.21.1
krb5-debugsource-1.11.3-3.21.1
krb5-32bit-1.11.3-3.21.1
krb5-client-1.11.3-3.21.1
krb5-server-debuginfo-1.11.3-3.21.1
krb5-devel-1.11.3-3.21.1
krb5-mini-debugsource-1.11.3-3.21.1
krb5-devel-32bit-1.11.3-3.21.1

i586
krb5-mini-debuginfo-1.11.3-3.21.1
krb5-debuginfo-1.11.3-3.21.1
krb5-doc-1.11.3-3.21.1
krb5-plugin-preauth-pkinit-1.11.3-3.21.1
krb5-1.11.3-3.21.1
krb5-plugin-preauth-pkinit-debuginfo-1.11.3-3.21.1
krb5-plugin-kdb-ldap-debuginfo-1.11.3-3.21.1
krb5-plugin-kdb-ldap-1.11.3-3.21.1
krb5-client-debuginfo-1.11.3-3.21.1
krb5-mini-devel-1.11.3-3.21.1
krb5-mini-1.11.3-3.21.1
krb5-server-1.11.3-3.21.1
krb5-debugsource-1.11.3-3.21.1
krb5-client-1.11.3-3.21.1
krb5-server-debuginfo-1.11.3-3.21.1
krb5-devel-1.11.3-3.21.1
krb5-mini-debugsource-1.11.3-3.21.1

SuSE Linux 13.2
x86_64
krb5-plugin-preauth-otp-1.12.2-15.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.2-15.1
krb5-server-1.12.2-15.1
krb5-plugin-preauth-otp-debuginfo-1.12.2-15.1
krb5-mini-debugsource-1.12.2-15.1
krb5-plugin-kdb-ldap-debuginfo-1.12.2-15.1
krb5-debuginfo-1.12.2-15.1
krb5-devel-32bit-1.12.2-15.1
krb5-client-1.12.2-15.1
krb5-client-debuginfo-1.12.2-15.1
krb5-devel-1.12.2-15.1
krb5-mini-devel-1.12.2-15.1
krb5-mini-debuginfo-1.12.2-15.1
krb5-1.12.2-15.1
krb5-doc-1.12.2-15.1
krb5-debuginfo-32bit-1.12.2-15.1

krb5-debugsource-1.12.2-15.1
krb5-server-debuginfo-1.12.2-15.1
krb5-plugin-kdb-ldap-1.12.2-15.1
krb5-plugin-preauth-pkinit-1.12.2-15.1
krb5-mini-1.12.2-15.1
krb5-32bit-1.12.2-15.1

i586
krb5-plugin-preauth-otp-1.12.2-15.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.2-15.1
krb5-server-1.12.2-15.1
krb5-plugin-preauth-otp-debuginfo-1.12.2-15.1
krb5-mini-debugsource-1.12.2-15.1
krb5-plugin-kdb-ldap-debuginfo-1.12.2-15.1
krb5-debuginfo-1.12.2-15.1
krb5-client-1.12.2-15.1
krb5-client-debuginfo-1.12.2-15.1
krb5-devel-1.12.2-15.1
krb5-mini-devel-1.12.2-15.1
krb5-mini-debuginfo-1.12.2-15.1
krb5-1.12.2-15.1
krb5-doc-1.12.2-15.1
krb5-debugsource-1.12.2-15.1
krb5-server-debuginfo-1.12.2-15.1
krb5-plugin-kdb-ldap-1.12.2-15.1
krb5-plugin-preauth-pkinit-1.12.2-15.1
krb5-mini-1.12.2-15.1

144035 - SuSE Linux 13.1 openSUSE-SU-2015:1920-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1920-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00041.html

SuSE Linux 13.1
x86_64
wpa_supplicant-debugsource-2.0-3.17.1
wpa_supplicant-gui-debuginfo-2.0-3.17.1
wpa_supplicant-gui-2.0-3.17.1
wpa_supplicant-2.0-3.17.1
wpa_supplicant-debuginfo-2.0-3.17.1

i586
wpa_supplicant-debugsource-2.0-3.17.1
wpa_supplicant-gui-debuginfo-2.0-3.17.1
wpa_supplicant-gui-2.0-3.17.1
wpa_supplicant-2.0-3.17.1
wpa_supplicant-debuginfo-2.0-3.17.1

144037 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1942-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-4514, CVE-2015-4515, CVE-2015-4518, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7185, CVE-2015-7186, CVE-2015-7187, CVE-2015-7188, CVE-2015-7189, CVE-2015-7190, CVE-2015-7191, CVE-2015-7192, CVE-2015-7193, CVE-2015-7194, CVE-2015-7195, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1942-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00051.html

SuSE Linux 13.1
x86_64
mozilla-nspr-debugsource-4.10.10-25.1
seamonkey-2.39-59.1
libsoftokn3-debuginfo-3.20.1-62.2
libfreebl3-debuginfo-3.20.1-62.2
MozillaFirefox-translations-other-42.0-94.4
libsoftokn3-3.20.1-62.2
mozilla-nss-sysinit-debuginfo-32bit-3.20.1-62.2
libfreebl3-debuginfo-32bit-3.20.1-62.2
MozillaFirefox-buildsymbols-42.0-94.4
mozilla-nss-tools-3.20.1-62.2
mozilla-nss-sysinit-32bit-3.20.1-62.2
mozilla-nss-devel-3.20.1-62.2
MozillaFirefox-branding-upstream-42.0-94.4
mozilla-nspr-4.10.10-25.1
MozillaFirefox-devel-42.0-94.4
seamonkey-debugsource-2.39-59.1
seamonkey-translations-other-2.39-59.1
mozilla-nss-certs-debuginfo-3.20.1-62.2
mozilla-nss-debugsource-3.20.1-62.2
mozilla-nss-certs-debuginfo-32bit-3.20.1-62.2
mozilla-nss-32bit-3.20.1-62.2
mozilla-nspr-debuginfo-32bit-4.10.10-25.1
MozillaFirefox-translations-common-42.0-94.4
libfreebl3-32bit-3.20.1-62.2
MozillaFirefox-debugsource-42.0-94.4
mozilla-nss-3.20.1-62.2
mozilla-nss-debuginfo-32bit-3.20.1-62.2
mozilla-nspr-debuginfo-4.10.10-25.1
libsoftokn3-32bit-3.20.1-62.2
seamonkey-dom-inspector-2.39-59.1
seamonkey-translations-common-2.39-59.1
mozilla-nss-certs-3.20.1-62.2
mozilla-nspr-devel-4.10.10-25.1
libfreebl3-3.20.1-62.2
seamonkey-irc-2.39-59.1
mozilla-nspr-32bit-4.10.10-25.1
mozilla-nss-sysinit-debuginfo-3.20.1-62.2

libsoftokn3-debuginfo-32bit-3.20.1-62.2
mozilla-nss-tools-debuginfo-3.20.1-62.2
seamonkey-debuginfo-2.39-59.1
MozillaFirefox-42.0-94.4
MozillaFirefox-debuginfo-42.0-94.4
mozilla-nss-certs-32bit-3.20.1-62.2
mozilla-nss-sysinit-3.20.1-62.2
mozilla-nss-debuginfo-3.20.1-62.2

i586
mozilla-nspr-debugsource-4.10.10-25.1
seamonkey-2.39-59.1
libsoftokn3-debuginfo-3.20.1-62.2
libfreebl3-debuginfo-3.20.1-62.2
MozillaFirefox-translations-other-42.0-94.4
libsoftokn3-3.20.1-62.2
MozillaFirefox-buildsymbols-42.0-94.4
mozilla-nss-tools-3.20.1-62.2
mozilla-nss-devel-3.20.1-62.2
MozillaFirefox-branding-upstream-42.0-94.4
mozilla-nspr-4.10.10-25.1
MozillaFirefox-devel-42.0-94.4
seamonkey-debugsource-2.39-59.1
seamonkey-translations-other-2.39-59.1
mozilla-nss-certs-debuginfo-3.20.1-62.2
mozilla-nss-debugsource-3.20.1-62.2
MozillaFirefox-translations-common-42.0-94.4
MozillaFirefox-debugsource-42.0-94.4
mozilla-nss-3.20.1-62.2
mozilla-nspr-debuginfo-4.10.10-25.1
seamonkey-dom-inspector-2.39-59.1
seamonkey-translations-common-2.39-59.1
mozilla-nss-certs-3.20.1-62.2
mozilla-nspr-devel-4.10.10-25.1
libfreebl3-3.20.1-62.2
seamonkey-irc-2.39-59.1
mozilla-nss-sysinit-debuginfo-3.20.1-62.2
mozilla-nss-tools-debuginfo-3.20.1-62.2
seamonkey-debuginfo-2.39-59.1
MozillaFirefox-42.0-94.4
MozillaFirefox-debuginfo-42.0-94.4
mozilla-nss-sysinit-3.20.1-62.2
mozilla-nss-debuginfo-3.20.1-62.2

SuSE Linux 13.2
x86_64
MozillaFirefox-debugsource-42.0-50.4
MozillaFirefox-branding-upstream-42.0-50.4
MozillaFirefox-debuginfo-42.0-50.4
mozilla-nss-certs-3.20.1-19.2
MozillaFirefox-translations-common-42.0-50.4
seamonkey-translations-common-2.39-23.1
libsoftokn3-debuginfo-32bit-3.20.1-19.2
mozilla-nspr-32bit-4.10.10-9.1
mozilla-nss-3.20.1-19.2
MozillaFirefox-buildsymbols-42.0-50.4
mozilla-nss-sysinit-debuginfo-32bit-3.20.1-19.2
libsoftokn3-32bit-3.20.1-19.2
libsoftokn3-debuginfo-3.20.1-19.2
seamonkey-dom-inspector-2.39-23.1

libfreebl3-debuginfo-3.20.1-19.2
mozilla-nspr-debuginfo-32bit-4.10.10-9.1
mozilla-nss-tools-debuginfo-3.20.1-19.2
libfreebl3-32bit-3.20.1-19.2
mozilla-nss-debuginfo-3.20.1-19.2
mozilla-nspr-devel-4.10.10-9.1
mozilla-nspr-debugsource-4.10.10-9.1
seamonkey-translations-other-2.39-23.1
mozilla-nss-sysinit-32bit-3.20.1-19.2
mozilla-nss-sysinit-3.20.1-19.2
mozilla-nss-certs-32bit-3.20.1-19.2
mozilla-nss-sysinit-debuginfo-3.20.1-19.2
mozilla-nss-32bit-3.20.1-19.2
libsoftokn3-3.20.1-19.2
MozillaFirefox-devel-42.0-50.4
mozilla-nss-devel-3.20.1-19.2
mozilla-nspr-4.10.10-9.1
seamonkey-2.39-23.1
mozilla-nss-certs-debuginfo-32bit-3.20.1-19.2
libfreebl3-3.20.1-19.2
mozilla-nss-tools-3.20.1-19.2
MozillaFirefox-42.0-50.4
mozilla-nss-debuginfo-32bit-3.20.1-19.2
mozilla-nss-debugsource-3.20.1-19.2
seamonkey-debuginfo-2.39-23.1
mozilla-nss-certs-debuginfo-3.20.1-19.2
seamonkey-debugsource-2.39-23.1
mozilla-nspr-debuginfo-4.10.10-9.1
libfreebl3-debuginfo-32bit-3.20.1-19.2
seamonkey-irc-2.39-23.1
MozillaFirefox-translations-other-42.0-50.4

i586
MozillaFirefox-debugsource-42.0-50.4
MozillaFirefox-branding-upstream-42.0-50.4
MozillaFirefox-debuginfo-42.0-50.4
mozilla-nss-certs-3.20.1-19.2
MozillaFirefox-translations-common-42.0-50.4
seamonkey-translations-common-2.39-23.1
mozilla-nss-3.20.1-19.2
MozillaFirefox-buildsymbols-42.0-50.4
libsoftokn3-debuginfo-3.20.1-19.2
seamonkey-dom-inspector-2.39-23.1
libfreebl3-debuginfo-3.20.1-19.2
mozilla-nss-tools-debuginfo-3.20.1-19.2
mozilla-nss-debuginfo-3.20.1-19.2
mozilla-nspr-devel-4.10.10-9.1
mozilla-nspr-debugsource-4.10.10-9.1
seamonkey-translations-other-2.39-23.1
mozilla-nss-sysinit-3.20.1-19.2
mozilla-nss-sysinit-debuginfo-3.20.1-19.2
libsoftokn3-3.20.1-19.2
MozillaFirefox-devel-42.0-50.4
mozilla-nss-devel-3.20.1-19.2
mozilla-nspr-4.10.10-9.1
seamonkey-2.39-23.1
libfreebl3-3.20.1-19.2
mozilla-nss-tools-3.20.1-19.2
MozillaFirefox-42.0-50.4
mozilla-nss-debugsource-3.20.1-19.2

seamonkey-debuginfo-2.39-23.1
mozilla-nss-certs-debuginfo-3.20.1-19.2
seamonkey-debugsource-2.39-23.1
mozilla-nspr-debuginfo-4.10.10-9.1
seamonkey-irc-2.39-23.1
MozillaFirefox-translations-other-42.0-50.4

144040 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1913-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9680

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1913-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00038.html

SuSE Linux 13.1
x86_64
sudo-debuginfo-1.8.10p3-5.16.1
sudo-1.8.10p3-5.16.1
sudo-debugsource-1.8.10p3-5.16.1
sudo-devel-1.8.10p3-5.16.1

i586
sudo-debuginfo-1.8.10p3-5.16.1
sudo-1.8.10p3-5.16.1
sudo-debugsource-1.8.10p3-5.16.1
sudo-devel-1.8.10p3-5.16.1

SuSE Linux 13.2
x86_64
sudo-devel-1.8.10p3-2.7.1
sudo-1.8.10p3-2.7.1
sudo-debuginfo-1.8.10p3-2.7.1
sudo-debugsource-1.8.10p3-2.7.1
sudo-test-1.8.10p3-2.7.1

i586
sudo-devel-1.8.10p3-2.7.1
sudo-1.8.10p3-2.7.1
sudo-debuginfo-1.8.10p3-2.7.1
sudo-debugsource-1.8.10p3-2.7.1
sudo-test-1.8.10p3-2.7.1

144041 - SuSE Linux 13.2 openSUSE-SU-2015:1912-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1912-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00037.html

SuSE Linux 13.2
x86_64
wpa_supplicant-debugsource-2.2-5.10.1
wpa_supplicant-debuginfo-2.2-5.10.1
wpa_supplicant-2.2-5.10.1
wpa_supplicant-gui-debuginfo-2.2-5.10.1
wpa_supplicant-gui-2.2-5.10.1

i586
wpa_supplicant-debugsource-2.2-5.10.1
wpa_supplicant-debuginfo-2.2-5.10.1
wpa_supplicant-2.2-5.10.1
wpa_supplicant-gui-debuginfo-2.2-5.10.1
wpa_supplicant-gui-2.2-5.10.1

144042 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1897-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2695, CVE-2015-2696, CVE-2015-2697

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1897-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001666.html

SuSE SLED 12
x86_64
krb5-32bit-1.12.1-19.1
krb5-debuginfo-1.12.1-19.1
krb5-debugsource-1.12.1-19.1
krb5-client-debuginfo-1.12.1-19.1
krb5-debuginfo-32bit-1.12.1-19.1
krb5-client-1.12.1-19.1
krb5-1.12.1-19.1

SuSE SLES 12
x86_64
krb5-plugin-preauth-otp-debuginfo-1.12.1-19.1
krb5-1.12.1-19.1
krb5-plugin-kdb-ldap-debuginfo-1.12.1-19.1
krb5-plugin-kdb-ldap-1.12.1-19.1

krb5-client-1.12.1-19.1
krb5-plugin-preauth-otp-1.12.1-19.1
krb5-debugsource-1.12.1-19.1
krb5-debuginfo-1.12.1-19.1
krb5-doc-1.12.1-19.1
krb5-plugin-preauth-pkinit-1.12.1-19.1
krb5-32bit-1.12.1-19.1
krb5-client-debuginfo-1.12.1-19.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.1-19.1
krb5-debuginfo-32bit-1.12.1-19.1
krb5-server-1.12.1-19.1
krb5-server-debuginfo-1.12.1-19.1

144043 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1915-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147, CVE-2015-1774, CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1915-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2015-November/001669.html

SuSE SLED 12
x86_64
librevenge-stream-0_0-0-0.0.2-4.1
liborcus-0_8-0-debuginfo-0.7.1-3.1
libodfgen-0_1-1-0.1.4-3.9
libreoffice-impress-debuginfo-5.0.2.2-13.14
libpagemaker-0_0-0-debuginfo-0.0.2-2.3
libreoffice-5.0.2.2-13.14
libreoffice-base-drivers-postgresql-5.0.2.2-13.14
libgltf-0_0-0-debuginfo-0.0.1-2.1
libvoikko1-3.7.1-3.1
libe-book-0_1-1-debuginfo-0.1.2-4.2
libreoffice-voikko-debuginfo-4.1-6.3
libreoffice-filters-optional-5.0.2.2-13.14
libfreehand-0_1-1-0.1.1-4.9
libixion-debugsource-0.9.1-3.1
libreoffice-base-debuginfo-5.0.2.2-13.14
librevenge-0_0-0-debuginfo-0.0.2-4.1
libgraphite2-3-debuginfo-32bit-1.3.1-3.1
libvoikko-debugsource-3.7.1-3.1
hyphen-debugsource-2.8.8-9.1
libreoffice-writer-debuginfo-5.0.2.2-13.14
libreoffice-draw-5.0.2.2-13.14
libe-book-0_1-1-0.1.2-4.2
libreoffice-writer-extensions-5.0.2.2-13.14
librevenge-0_0-0-0.0.2-4.1
graphite2-debugsource-1.3.1-3.1
libreoffice-voikko-4.1-6.3
libcmis-0_5-5-0.5.0-5.1

libfreehand-debugsource-0.1.1-4.9
libpagemaker-0_0-0-0.0.2-2.3
libwps-0_4-4-0.4.1-3.1
libreoffice-impress-5.0.2.2-13.14
libcdr-debugsource-0.1.1-5.3
liblangtag1-0.5.7-3.1
libgltf-debugsource-0.0.1-2.1
libcmis-0_5-5-debuginfo-0.5.0-5.1
libgraphite2-3-debuginfo-1.3.1-3.1
libreoffice-calc-5.0.2.2-13.14
libreoffice-gnome-5.0.2.2-13.14
libreoffice-debuginfo-5.0.2.2-13.14
libvisio-debugsource-0.1.3-4.3
libreoffice-draw-debuginfo-5.0.2.2-13.14
libetonyek-0_1-1-debuginfo-0.1.3-3.5
libreoffice-math-5.0.2.2-13.14
libreoffice-pyuno-debuginfo-5.0.2.2-13.14
libixion-0_10-0-0.9.1-3.1
libreoffice-base-drivers-mysql-5.0.2.2-13.14
libpagemaker-debugsource-0.0.2-2.3
libabw-debugsource-0.1.1-5.3
libreoffice-debugsource-5.0.2.2-13.14
libetonyek-0_1-1-0.1.3-3.5
libcdr-0_1-1-0.1.1-5.3
libreoffice-gnome-debuginfo-5.0.2.2-13.14
libfreehand-0_1-1-debuginfo-0.1.1-4.9
cmis-client-debuginfo-0.5.0-5.1
liborcus-debugsource-0.7.1-3.1
libreoffice-calc-extensions-5.0.2.2-13.14
graphite2-debuginfo-1.3.1-3.1
libgraphite2-3-1.3.1-3.1
libmspub-0_1-1-debuginfo-0.1.2-5.1
libreoffice-base-5.0.2.2-13.14
libmwaw-0_3-3-debuginfo-0.3.6-3.3
cmis-client-debugsource-0.5.0-5.1
libmwaw-debugsource-0.3.6-3.3
librevenge-stream-0_0-0-debuginfo-0.0.2-4.1
libreoffice-calc-debuginfo-5.0.2.2-13.14
libwps-0_4-4-debuginfo-0.4.1-3.1
libgltf-0_0-0-0.0.1-2.1
libmspub-debugsource-0.1.2-5.1
libreoffice-mailmerge-5.0.2.2-13.14
libreoffice-base-drivers-postgresql-debuginfo-5.0.2.2-13.14
libodfgen-debugsource-0.1.4-3.9
libcdr-0_1-1-debuginfo-0.1.1-5.3
libreoffice-base-drivers-mysql-debuginfo-5.0.2.2-13.14
libmspub-0_1-1-0.1.2-5.1
libodfgen-0_1-1-debuginfo-0.1.4-3.9
libetonyek-debugsource-0.1.3-3.5
libwps-debugsource-0.4.1-3.1
libreoffice-math-debuginfo-5.0.2.2-13.14
libixion-0_10-0-debuginfo-0.9.1-3.1
libvoikko1-debuginfo-3.7.1-3.1
libhyphen0-debuginfo-2.8.8-9.1
libmwaw-0_3-3-0.3.6-3.3
libabw-0_1-1-debuginfo-0.1.1-5.3
libgraphite2-3-32bit-1.3.1-3.1
libvisio-0_1-1-debuginfo-0.1.3-4.3
librevenge-debugsource-0.0.2-4.1
libvisio-0_1-1-0.1.3-4.3

libreoffice-pyuno-5.0.2.2-13.14
myspell-dictionaries-20150827-5.1
libreoffice-officebean-debuginfo-5.0.2.2-13.14
libreoffice-writer-5.0.2.2-13.14
liblangtag1-debuginfo-0.5.7-3.1
liblangtag-debugsource-0.5.7-3.1
liborcus-0_8-0-0.7.1-3.1
libe-book-debugsource-0.1.2-4.2
libreoffice-officebean-5.0.2.2-13.14
libabw-0_1-1-0.1.1-5.3
libhyphen0-2.8.8-9.1

noarch
myspell-vi-20150827-5.1
myspell-fr_FR-20150827-5.1
libreoffice-l10n-zu-5.0.2.2-13.14
libreoffice-l10n-nn-5.0.2.2-13.14
libreoffice-l10n-ar-5.0.2.2-13.14
libreoffice-l10n-xh-5.0.2.2-13.14
myspell-ar-20150827-5.1
myspell-bg_BG-20150827-5.1
libreoffice-l10n-zh-Hans-5.0.2.2-13.14
libreoffice-l10n-nb-5.0.2.2-13.14
myspell-sr-20150827-5.1
libreoffice-l10n-pt-BR-5.0.2.2-13.14
libreoffice-l10n-en-5.0.2.2-13.14
libreoffice-l10n-zh-Hant-5.0.2.2-13.14
myspell-pl_PL-20150827-5.1
myspell-he_IL-20150827-5.1
libreoffice-l10n-cs-5.0.2.2-13.14
myspell-nl_NL-20150827-5.1
myspell-sv_SE-20150827-5.1
myspell-el_GR-20150827-5.1
myspell-es-20150827-5.1
myspell-hi_IN-20150827-5.1
libformula-1.1.3-4.3
libreoffice-l10n-fi-5.0.2.2-13.14
myspell-ru_RU-20150827-5.1
libreoffice-l10n-da-5.0.2.2-13.14
libreoffice-l10n-hi-5.0.2.2-13.14
libreoffice-l10n-fr-5.0.2.2-13.14
myspell-hr_HR-20150827-5.1
liblayout-0.2.10-4.8
myspell-no-20150827-5.1
libreoffice-l10n-it-5.0.2.2-13.14
pentaho-reporting-flow-engine-0.9.4-4.5
libserializer-1.1.2-4.3
myspell-en-20150827-5.1
myspell-lv_LV-20150827-5.1
myspell-ca-20150827-5.1
libreoffice-l10n-de-5.0.2.2-13.14
myspell-te_IN-20150827-5.1
libreoffice-l10n-sk-5.0.2.2-13.14
myspell-ro-20150827-5.1
myspell-sl_SI-20150827-5.1
libreoffice-l10n-es-5.0.2.2-13.14
flute-1.3.0-4.2
myspell-da_DK-20150827-5.1
myspell-cs_CZ-20150827-5.1
libreoffice-l10n-ca-5.0.2.2-13.14

malaga-suomi-1.18-3.2
libfonts-1.1.3-4.9
sac-1.3-4.1
librepository-1.1.3-4.3
myspell-de-20150827-5.1
libreoffice-l10n-pt-PT-5.0.2.2-13.14
myspell-zu_ZA-20150827-5.1
myspell-lo_LA-20150827-5.1
libreoffice-icon-theme-tango-5.0.2.2-13.14
pentaho-libxml-1.1.3-4.3
myspell-af_ZA-20150827-5.1
myspell-lt_LT-20150827-5.1
myspell-bs_BA-20150827-5.1
libreoffice-l10n-gu-5.0.2.2-13.14
libreoffice-l10n-af-5.0.2.2-13.14
libreoffice-l10n-nl-5.0.2.2-13.14
libbase-1.1.3-4.3
myspell-bn_BD-20150827-5.1
myspell-gu_IN-20150827-5.1
libreoffice-l10n-ja-5.0.2.2-13.14
myspell-pt_PT-20150827-5.1
myspell-it_IT-20150827-5.1
myspell-be_BY-20150827-5.1
libloader-1.1.3-3.2
libreoffice-l10n-ko-5.0.2.2-13.14
myspell-th_TH-20150827-5.1
myspell-hu_HU-20150827-5.1
apache-commons-logging-1.1.3-7.1
myspell-sk_SK-20150827-5.1
libreoffice-l10n-hu-5.0.2.2-13.14
myspell-pt_BR-20150827-5.1
libreoffice-l10n-sv-5.0.2.2-13.14
libreoffice-l10n-ru-5.0.2.2-13.14
libreoffice-l10n-pl-5.0.2.2-13.14
libreoffice-share-linker-1-2.1
myspell-et_EE-20150827-5.1

SuSE SLES 12
noarch
apache-commons-logging-1.1.3-7.1

x86_64
libgraphite2-3-debuginfo-1.3.1-3.1
libgraphite2-3-1.3.1-3.1
libgraphite2-3-debuginfo-32bit-1.3.1-3.1
graphite2-debugsource-1.3.1-3.1
graphite2-debuginfo-1.3.1-3.1
libgraphite2-3-32bit-1.3.1-3.1

170585 - Amazon Linux AMI ALAS-2015-608 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ALAS-2015-608

Observation

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

https://alas.aws.amazon.com/ALAS-2015-608.html

Amazon Linux AMI
x86_64
nss-sysinit-3.19.1-7.74.amzn1
nspr-debuginfo-4.10.8-2.35.amzn1
nss-devel-3.19.1-7.74.amzn1
nspr-devel-4.10.8-2.35.amzn1
nss-util-3.19.1-4.47.amzn1
nss-3.19.1-7.74.amzn1
nss-util-devel-3.19.1-4.47.amzn1
nss-tools-3.19.1-7.74.amzn1
jss-4.2.6-35.17.amzn1
nss-util-debuginfo-3.19.1-4.47.amzn1
nspr-4.10.8-2.35.amzn1
nss-pkcs11-devel-3.19.1-7.74.amzn1
nss-debuginfo-3.19.1-7.74.amzn1
jss-debuginfo-4.2.6-35.17.amzn1
jss-javadoc-4.2.6-35.17.amzn1

i686
nss-sysinit-3.19.1-7.74.amzn1
nspr-debuginfo-4.10.8-2.35.amzn1
nss-devel-3.19.1-7.74.amzn1
nspr-devel-4.10.8-2.35.amzn1
nss-util-3.19.1-4.47.amzn1
nss-3.19.1-7.74.amzn1
nss-util-devel-3.19.1-4.47.amzn1
nss-tools-3.19.1-7.74.amzn1
jss-4.2.6-35.17.amzn1
nss-util-debuginfo-3.19.1-4.47.amzn1
nspr-4.10.8-2.35.amzn1
nss-pkcs11-devel-3.19.1-7.74.amzn1
nss-debuginfo-3.19.1-7.74.amzn1
jss-debuginfo-4.2.6-35.17.amzn1
jss-javadoc-4.2.6-35.17.amzn1

185040 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2785-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-4514, CVE-2015-4515, CVE-2015-4518, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7187, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7195, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

Description

The scan detected that the host is missing the following update:
USN-2785-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003172.html

Ubuntu 12.04

firefox_42.0+build2-0ubuntu0.12.04.1

Ubuntu 15.04

firefox_42.0+build2-0ubuntu0.15.04.1

Ubuntu 15.10

firefox_42.0+build2-0ubuntu0.15.10.1

Ubuntu 14.04

firefox_42.0+build2-0ubuntu0.14.04.1

185041 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2791-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-2791-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003171.html

Ubuntu 12.04

libnss3_3.19.2.1-0ubuntu0.12.04.1

Ubuntu 15.04

libnss3_3.19.2.1-0ubuntu0.15.04.1

Ubuntu 15.10

libnss3_3.19.2.1-0ubuntu0.15.10.1

Ubuntu 14.04

libnss3_3.19.2.1-0ubuntu0.14.04.1

185052 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2790-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7183

Description

The scan detected that the host is missing the following update:
USN-2790-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003170.html

Ubuntu 12.04

libnspr4_4.10.10-0ubuntu0.12.04.1

Ubuntu 15.04

libnspr4_4.10.10-0ubuntu0.15.04.1

Ubuntu 15.10

libnspr4_4.10.10-0ubuntu0.15.10.1

Ubuntu 14.04

libnspr4_4.10.10-0ubuntu0.14.04.1

189920 - Fedora Linux 23 FEDORA-2015-a931b02be2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7812, CVE-2015-7813, CVE-2015-7814, CVE-2015-7835, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a931b02be2

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171082.html

Fedora Core 23

xen-4.5.1-14.fc23

189922 - Fedora Linux 21 FEDORA-2015-242be2c240 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7812, CVE-2015-7813, CVE-2015-7814, CVE-2015-7835, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2015-242be2c240

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171249.html

Fedora Core 21

xen-4.4.3-7.fc21

189947 - Fedora Linux 22 FEDORA-2015-6f6b79efe2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7812, CVE-2015-7813, CVE-2015-7814, CVE-2015-7835, CVE-2015-7969, CVE-2015-7970, CVE-2015-7971, CVE-2015-7972

Description

The scan detected that the host is missing the following update:
FEDORA-2015-6f6b79efe2

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171185.html

Fedora Core 22

xen-4.5.1-14.fc22

85998 - CentOS 7 CESA-2015-1978 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8559, CVE-2015-5156

Description

The scan detected that the host is missing the following update:
CESA-2015-1978

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021463.html

CentOS 7
x86_64
kernel-debug-3.10.0-229.20.1.el7
perf-3.10.0-229.20.1.el7
kernel-tools-3.10.0-229.20.1.el7
kernel-debug-devel-3.10.0-229.20.1.el7
kernel-tools-libs-devel-3.10.0-229.20.1.el7

kernel-devel-3.10.0-229.20.1.el7
python-perf-3.10.0-229.20.1.el7
kernel-tools-libs-3.10.0-229.20.1.el7
kernel-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7

noarch
kernel-doc-3.10.0-229.20.1.el7
kernel-abi-whitelists-3.10.0-229.20.1.el7

91923 - Oracle Enterprise Linux ELSA-2015-3092 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5156

Description

The scan detected that the host is missing the following update:
ELSA-2015-3092

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005496.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005497.html

OEL7
x86_64
kernel-uek-firmware-3.8.13-98.5.2.el7uek
kernel-uek-devel-3.8.13-98.5.2.el7uek
kernel-uek-debug-3.8.13-98.5.2.el7uek
kernel-uek-debug-devel-3.8.13-98.5.2.el7uek
kernel-uek-doc-3.8.13-98.5.2.el7uek
dtrace-modules-3.8.13-98.5.2.el7uek-0.4.5-3.el7
kernel-uek-3.8.13-98.5.2.el7uek

OEL6
x86_64
kernel-uek-firmware-3.8.13-98.5.2.el6uek
dtrace-modules-3.8.13-98.5.2.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-98.5.2.el6uek
kernel-uek-3.8.13-98.5.2.el6uek
kernel-uek-debug-3.8.13-98.5.2.el6uek
kernel-uek-doc-3.8.13-98.5.2.el6uek
kernel-uek-devel-3.8.13-98.5.2.el6uek

91924 - Oracle Enterprise Linux ELSA-2015-2019 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

The scan detected that the host is missing the following update:
ELSA-2015-2019

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005530.html

OEL6
x86_64
sssd-proxy-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
bsss_idmap-devel-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
libsss_nss_idmap-1.12.4-47.el6_7.4
python-sssdconfig-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

i386
sssd-proxy-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
libsss_nss_idmap-1.12.4-47.el6_7.4
python-sssdconfig-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

91925 - Oracle Enterprise Linux ELSA-2015-3094 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5156

Description

The scan detected that the host is missing the following update:
ELSA-2015-3094

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005500.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005499.html

OEL5
x86_64
kernel-uek-debug-devel-2.6.32-400.37.12.el5uek
mlnx_en-2.6.32-400.37.12.el5uek-1.5.7-2
ofa-2.6.32-400.37.12.el5uek-1.5.1-4.0.58
kernel-uek-devel-2.6.32-400.37.12.el5uek
kernel-uek-debug-2.6.32-400.37.12.el5uek
kernel-uek-2.6.32-400.37.12.el5uek
kernel-uek-doc-2.6.32-400.37.12.el5uek
ofa-2.6.32-400.37.12.el5uekdebug-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.12.el5uekdebug-1.5.7-2
kernel-uek-firmware-2.6.32-400.37.12.el5uek

i386
kernel-uek-doc-2.6.32-400.37.12.el5uek
mlnx_en-2.6.32-400.37.12.el5uek-1.5.7-2
ofa-2.6.32-400.37.12.el5uek-1.5.1-4.0.58
kernel-uek-devel-2.6.32-400.37.12.el5uek
kernel-uek-debug-2.6.32-400.37.12.el5uek
kernel-uek-2.6.32-400.37.12.el5uek
kernel-uek-debug-devel-2.6.32-400.37.12.el5uek
ofa-2.6.32-400.37.12.el5uekdebug-1.5.1-4.0.58
mlnx_en-2.6.32-400.37.12.el5uekdebug-1.5.7-2
kernel-uek-firmware-2.6.32-400.37.12.el5uek

OEL6
x86_64
kernel-uek-debug-2.6.32-400.37.12.el6uek
ofa-2.6.32-400.37.12.el6uek-1.5.1-4.0.58
kernel-uek-2.6.32-400.37.12.el6uek
kernel-uek-firmware-2.6.32-400.37.12.el6uek
ofa-2.6.32-400.37.12.el6uekdebug-1.5.1-4.0.58
kernel-uek-doc-2.6.32-400.37.12.el6uek
mlnx_en-2.6.32-400.37.12.el6uekdebug-1.5.7-0.1
kernel-uek-debug-devel-2.6.32-400.37.12.el6uek
mlnx_en-2.6.32-400.37.12.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.37.12.el6uek

i386
kernel-uek-debug-2.6.32-400.37.12.el6uek
ofa-2.6.32-400.37.12.el6uek-1.5.1-4.0.58
kernel-uek-2.6.32-400.37.12.el6uek
kernel-uek-firmware-2.6.32-400.37.12.el6uek

ofa-2.6.32-400.37.12.el6uekdebug-1.5.1-4.0.58
kernel-uek-doc-2.6.32-400.37.12.el6uek
mlnx_en-2.6.32-400.37.12.el6uekdebug-1.5.7-0.1
kernel-uek-debug-devel-2.6.32-400.37.12.el6uek
mlnx_en-2.6.32-400.37.12.el6uek-1.5.7-0.1
kernel-uek-devel-2.6.32-400.37.12.el6uek

91926 - Oracle Enterprise Linux ELSA-2015-3093 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5156

Description

The scan detected that the host is missing the following update:
ELSA-2015-3093

Observation

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

http://oss.oracle.com/pipermail/el-errata/2015-November/005498.html
http://oss.oracle.com/pipermail/el-errata/2015-November/005501.html

OEL5
x86_64
kernel-uek-debug-2.6.39-400.264.5.el5uek
kernel-uek-devel-2.6.39-400.264.5.el5uek
kernel-uek-doc-2.6.39-400.264.5.el5uek
kernel-uek-debug-devel-2.6.39-400.264.5.el5uek
kernel-uek-2.6.39-400.264.5.el5uek
kernel-uek-firmware-2.6.39-400.264.5.el5uek

i386
kernel-uek-debug-2.6.39-400.264.5.el5uek
kernel-uek-devel-2.6.39-400.264.5.el5uek
kernel-uek-doc-2.6.39-400.264.5.el5uek
kernel-uek-debug-devel-2.6.39-400.264.5.el5uek
kernel-uek-2.6.39-400.264.5.el5uek
kernel-uek-firmware-2.6.39-400.264.5.el5uek

OEL6
x86_64
kernel-uek-doc-2.6.39-400.264.5.el6uek
kernel-uek-debug-devel-2.6.39-400.264.5.el6uek
kernel-uek-2.6.39-400.264.5.el6uek
kernel-uek-debug-2.6.39-400.264.5.el6uek
kernel-uek-devel-2.6.39-400.264.5.el6uek
kernel-uek-firmware-2.6.39-400.264.5.el6uek

i386
kernel-uek-doc-2.6.39-400.264.5.el6uek
kernel-uek-debug-devel-2.6.39-400.264.5.el6uek
kernel-uek-2.6.39-400.264.5.el6uek
kernel-uek-debug-2.6.39-400.264.5.el6uek
kernel-uek-devel-2.6.39-400.264.5.el6uek
kernel-uek-firmware-2.6.39-400.264.5.el6uek

96021 - CentOS 6 CESA-2015-2019 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

The scan detected that the host is missing the following update:
CESA-2015-2019

Observation

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

http://lists.centos.org/pipermail/centos-announce/2015-November/021498.html

CentOS 6
i686
sssd-proxy-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
libsss_nss_idmap-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

noarch
python-sssdconfig-1.12.4-47.el6_7.4

x86_64
sssd-proxy-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
libsss_nss_idmap-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4

libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

132196 - Oracle VM OVMSA-2015-0144 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5156

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0144

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2015-November/000375.html

OVM3.3
x86_64
kernel-uek-3.8.13-98.5.2.el6uek
kernel-uek-firmware-3.8.13-98.5.2.el6uek

140971 - Red Hat Enterprise Linux RHSA-2015-2019 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

Description

The scan detected that the host is missing the following update:
RHSA-2015-2019

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-2019.html

RHEL6D
i386
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4

libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

noarch
python-sssdconfig-1.12.4-47.el6_7.4

x86_64
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

RHEL6S
i386
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4

libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

noarch
python-sssdconfig-1.12.4-47.el6_7.4

x86_64
libsss_nss_idmap-1.12.4-47.el6_7.4
libsss_simpleifp-devel-1.12.4-47.el6_7.4
sssd-ad-1.12.4-47.el6_7.4
libsss_simpleifp-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
libsss_nss_idmap-devel-1.12.4-47.el6_7.4
sssd-tools-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
libsss_idmap-devel-1.12.4-47.el6_7.4
libipa_hbac-devel-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
libsss_nss_idmap-python-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

RHEL6WS
i386
sssd-ad-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

noarch
python-sssdconfig-1.12.4-47.el6_7.4

x86_64

sssd-ad-1.12.4-47.el6_7.4
sssd-ldap-1.12.4-47.el6_7.4
sssd-1.12.4-47.el6_7.4
libipa_hbac-1.12.4-47.el6_7.4
sssd-ipa-1.12.4-47.el6_7.4
libipa_hbac-python-1.12.4-47.el6_7.4
sssd-krb5-common-1.12.4-47.el6_7.4
sssd-krb5-1.12.4-47.el6_7.4
sssd-client-1.12.4-47.el6_7.4
sssd-dbus-1.12.4-47.el6_7.4
sssd-proxy-1.12.4-47.el6_7.4
libsss_idmap-1.12.4-47.el6_7.4
sssd-debuginfo-1.12.4-47.el6_7.4
sssd-common-pac-1.12.4-47.el6_7.4
sssd-common-1.12.4-47.el6_7.4

144030 - SuSE Linux 13.2 openSUSE-SU-2015:1907-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1907-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00033.html

SuSE Linux 13.2
i586
postgresql93-9.3.10-2.7.1
postgresql93-devel-debuginfo-9.3.10-2.7.1
libecpg6-9.3.10-2.7.1
postgresql93-plpython-debuginfo-9.3.10-2.7.1
postgresql93-debuginfo-9.3.10-2.7.1
postgresql93-server-debuginfo-9.3.10-2.7.1
postgresql93-debugsource-9.3.10-2.7.1
libpq5-debuginfo-9.3.10-2.7.1
postgresql93-pltcl-9.3.10-2.7.1
postgresql93-contrib-debuginfo-9.3.10-2.7.1
postgresql93-libs-debugsource-9.3.10-2.7.1
postgresql93-server-9.3.10-2.7.1
postgresql93-test-9.3.10-2.7.1
postgresql93-plperl-9.3.10-2.7.1
postgresql93-plperl-debuginfo-9.3.10-2.7.1
postgresql93-devel-9.3.10-2.7.1
postgresql93-contrib-9.3.10-2.7.1
libpq5-9.3.10-2.7.1
libecpg6-debuginfo-9.3.10-2.7.1
postgresql93-pltcl-debuginfo-9.3.10-2.7.1
postgresql93-plpython-9.3.10-2.7.1

noarch
postgresql93-docs-9.3.10-2.7.1

x86_64
postgresql93-9.3.10-2.7.1
postgresql93-devel-debuginfo-9.3.10-2.7.1
libecpg6-9.3.10-2.7.1
postgresql93-plpython-debuginfo-9.3.10-2.7.1
postgresql93-debuginfo-9.3.10-2.7.1
libpq5-debuginfo-32bit-9.3.10-2.7.1
postgresql93-server-debuginfo-9.3.10-2.7.1
postgresql93-debugsource-9.3.10-2.7.1
libecpg6-32bit-9.3.10-2.7.1
libpq5-debuginfo-9.3.10-2.7.1
postgresql93-pltcl-9.3.10-2.7.1
postgresql93-contrib-debuginfo-9.3.10-2.7.1
libecpg6-debuginfo-32bit-9.3.10-2.7.1
postgresql93-libs-debugsource-9.3.10-2.7.1
postgresql93-server-9.3.10-2.7.1
postgresql93-test-9.3.10-2.7.1
postgresql93-plperl-9.3.10-2.7.1
postgresql93-plperl-debuginfo-9.3.10-2.7.1
postgresql93-devel-9.3.10-2.7.1
postgresql93-contrib-9.3.10-2.7.1
libpq5-9.3.10-2.7.1
libecpg6-debuginfo-9.3.10-2.7.1
postgresql93-pltcl-debuginfo-9.3.10-2.7.1
libpq5-32bit-9.3.10-2.7.1
postgresql93-plpython-9.3.10-2.7.1

144036 - SuSE Linux 13.1 openSUSE-SU-2015:1919-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1919-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00040.html

SuSE Linux 13.1
i586
postgresql92-plpython-debuginfo-9.2.14-4.7.2
postgresql92-devel-9.2.14-4.7.1
postgresql92-devel-debuginfo-9.2.14-4.7.1
postgresql92-plperl-9.2.14-4.7.2
postgresql92-9.2.14-4.7.2
postgresql92-debugsource-9.2.14-4.7.2
postgresql92-contrib-debuginfo-9.2.14-4.7.2
libecpg6-debuginfo-9.2.14-4.7.1
postgresql92-pltcl-debuginfo-9.2.14-4.7.2
postgresql92-server-9.2.14-4.7.2
postgresql92-server-debuginfo-9.2.14-4.7.2
postgresql92-pltcl-9.2.14-4.7.2
libecpg6-9.2.14-4.7.1

libpq5-9.2.14-4.7.1
postgresql92-plpython-9.2.14-4.7.2
libpq5-debuginfo-9.2.14-4.7.1
postgresql92-debuginfo-9.2.14-4.7.2
postgresql92-libs-debugsource-9.2.14-4.7.1
postgresql92-plperl-debuginfo-9.2.14-4.7.2
postgresql92-contrib-9.2.14-4.7.2

noarch
postgresql92-docs-9.2.14-4.7.2

x86_64
postgresql92-plpython-debuginfo-9.2.14-4.7.2
postgresql92-devel-9.2.14-4.7.1
postgresql92-devel-debuginfo-9.2.14-4.7.1
libecpg6-debuginfo-32bit-9.2.14-4.7.1
postgresql92-plperl-9.2.14-4.7.2
postgresql92-9.2.14-4.7.2
postgresql92-debugsource-9.2.14-4.7.2
libecpg6-32bit-9.2.14-4.7.1
postgresql92-contrib-debuginfo-9.2.14-4.7.2
libecpg6-debuginfo-9.2.14-4.7.1
libpq5-debuginfo-32bit-9.2.14-4.7.1
postgresql92-pltcl-debuginfo-9.2.14-4.7.2
postgresql92-server-9.2.14-4.7.2
postgresql92-server-debuginfo-9.2.14-4.7.2
postgresql92-pltcl-9.2.14-4.7.2
libecpg6-9.2.14-4.7.1
libpq5-9.2.14-4.7.1
libpq5-32bit-9.2.14-4.7.1
postgresql92-plpython-9.2.14-4.7.2
libpq5-debuginfo-9.2.14-4.7.1
postgresql92-debuginfo-9.2.14-4.7.2
postgresql92-libs-debugsource-9.2.14-4.7.1
postgresql92-plperl-debuginfo-9.2.14-4.7.2
postgresql92-contrib-9.2.14-4.7.2

170586 - Amazon Linux AMI ALAS-2015-609 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Description

The scan detected that the host is missing the following update:
ALAS-2015-609

Observation

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

https://alas.aws.amazon.com/ALAS-2015-609.html

Amazon Linux AMI
x86_64
postgresql94-devel-9.4.5-1.63.amzn1
postgresql93-plpython27-9.3.10-1.60.amzn1
postgresql93-pltcl-9.3.10-1.60.amzn1

postgresql93-libs-9.3.10-1.60.amzn1
postgresql92-test-9.2.14-1.56.amzn1
postgresql94-9.4.5-1.63.amzn1
postgresql92-plpython27-9.2.14-1.56.amzn1
postgresql94-plpython27-9.4.5-1.63.amzn1
postgresql94-docs-9.4.5-1.63.amzn1
postgresql92-pltcl-9.2.14-1.56.amzn1
postgresql94-server-9.4.5-1.63.amzn1
postgresql93-plpython26-9.3.10-1.60.amzn1
postgresql94-plpython26-9.4.5-1.63.amzn1
postgresql92-docs-9.2.14-1.56.amzn1
postgresql94-libs-9.4.5-1.63.amzn1
postgresql92-plperl-9.2.14-1.56.amzn1
postgresql93-server-9.3.10-1.60.amzn1
postgresql92-server-compat-9.2.14-1.56.amzn1
postgresql93-docs-9.3.10-1.60.amzn1
postgresql94-plperl-9.4.5-1.63.amzn1
postgresql94-pltcl-9.4.5-1.63.amzn1
postgresql94-contrib-9.4.5-1.63.amzn1
postgresql94-test-9.4.5-1.63.amzn1
postgresql92-server-9.2.14-1.56.amzn1
postgresql92-9.2.14-1.56.amzn1
postgresql93-contrib-9.3.10-1.60.amzn1
postgresql93-test-9.3.10-1.60.amzn1
postgresql92-debuginfo-9.2.14-1.56.amzn1
postgresql92-contrib-9.2.14-1.56.amzn1
postgresql93-devel-9.3.10-1.60.amzn1
postgresql94-debuginfo-9.4.5-1.63.amzn1
postgresql93-debuginfo-9.3.10-1.60.amzn1
postgresql92-libs-9.2.14-1.56.amzn1
postgresql93-9.3.10-1.60.amzn1
postgresql92-devel-9.2.14-1.56.amzn1
postgresql92-plpython26-9.2.14-1.56.amzn1
postgresql93-plperl-9.3.10-1.60.amzn1

i686
postgresql94-devel-9.4.5-1.63.amzn1
postgresql93-plpython27-9.3.10-1.60.amzn1
postgresql93-pltcl-9.3.10-1.60.amzn1
postgresql93-libs-9.3.10-1.60.amzn1
postgresql92-test-9.2.14-1.56.amzn1
postgresql94-9.4.5-1.63.amzn1
postgresql92-plpython27-9.2.14-1.56.amzn1
postgresql94-plpython27-9.4.5-1.63.amzn1
postgresql94-docs-9.4.5-1.63.amzn1
postgresql92-pltcl-9.2.14-1.56.amzn1
postgresql94-server-9.4.5-1.63.amzn1
postgresql93-plpython26-9.3.10-1.60.amzn1
postgresql94-plpython26-9.4.5-1.63.amzn1
postgresql92-docs-9.2.14-1.56.amzn1
postgresql94-libs-9.4.5-1.63.amzn1
postgresql92-plperl-9.2.14-1.56.amzn1
postgresql93-server-9.3.10-1.60.amzn1
postgresql92-server-compat-9.2.14-1.56.amzn1
postgresql93-docs-9.3.10-1.60.amzn1
postgresql94-plperl-9.4.5-1.63.amzn1
postgresql94-pltcl-9.4.5-1.63.amzn1
postgresql94-contrib-9.4.5-1.63.amzn1
postgresql94-test-9.4.5-1.63.amzn1
postgresql92-server-9.2.14-1.56.amzn1

postgresql92-9.2.14-1.56.amzn1
postgresql93-contrib-9.3.10-1.60.amzn1
postgresql93-test-9.3.10-1.60.amzn1
postgresql92-debuginfo-9.2.14-1.56.amzn1
postgresql92-contrib-9.2.14-1.56.amzn1
postgresql93-devel-9.3.10-1.60.amzn1
postgresql94-debuginfo-9.4.5-1.63.amzn1
postgresql93-debuginfo-9.3.10-1.60.amzn1
postgresql92-libs-9.2.14-1.56.amzn1
postgresql93-9.3.10-1.60.amzn1
postgresql92-devel-9.2.14-1.56.amzn1
postgresql92-plpython26-9.2.14-1.56.amzn1
postgresql93-plperl-9.3.10-1.60.amzn1

181661 - FreeBSD libvpx Buffer Overflow In Vp9_init_context_buffers (6ca7eddd-d436-486a-b169-b948436bcf14)

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

Risk Level: Medium

CVE: CVE-2015-4506

Description

The scan detected that the host is missing the following update:
libvpx -- buffer overflow in vp9_init_context_buffers (6ca7eddd-d436-486a-b169-b948436bcf14)

Observation

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

http://www.vuxml.org/freebsd/6ca7eddd-d436-486a-b169-b948436bcf14.html

Affected packages:
libvpx < 1.4.0.488_1

185036 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2788-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7696, CVE-2015-7697

Description

The scan detected that the host is missing the following update:
USN-2788-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003181.html

Ubuntu 12.04

unzip_6.0-4ubuntu2.5

Ubuntu 15.04

unzip_6.0-13ubuntu3.2

Ubuntu 15.10

unzip_6.0-17ubuntu1.2

Ubuntu 14.04

unzip_6.0-9ubuntu1.5

185047 - Ubuntu Linux 12.04 USN-2796-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2925, CVE-2015-5257, CVE-2015-7613

Description

The scan detected that the host is missing the following update:
USN-2796-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003177.html

Ubuntu 12.04

linux-image-3.2.0-1473-omap4_3.2.0-1473.95

185054 - Ubuntu Linux 12.04 USN-2792-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2925, CVE-2015-5257, CVE-2015-7613

Description

The scan detected that the host is missing the following update:
USN-2792-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003174.html

Ubuntu 12.04

linux-image-3.2.0-93-generic_3.2.0-93.133
linux-image-3.2.0-93-powerpc64-smp_3.2.0-93.133
linux-image-3.2.0-93-virtual_3.2.0-93.133
linux-image-3.2.0-93-generic-pae_3.2.0-93.133
linux-image-3.2.0-93-powerpc-smp_3.2.0-93.133
linux-image-3.2.0-93-highbank_3.2.0-93.133
linux-image-3.2.0-93-omap_3.2.0-93.133

189919 - Fedora Linux 21 FEDORA-2015-f1e18131bc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5161, CVE-2015-5723

Description

The scan detected that the host is missing the following update:
FEDORA-2015-f1e18131bc

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171122.html

Fedora Core 21

php-ZendFramework-1.12.16-1.fc21

189921 - Fedora Linux 21 FEDORA-2015-97fe05f788 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8001, CVE-2015-8002, CVE-2015-8003, CVE-2015-8004, CVE-2015-8005, CVE-2015-8006, CVE-2015-8007, CVE-2015-8008, CVE-2015-8009

Description

The scan detected that the host is missing the following update:
FEDORA-2015-97fe05f788

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170961.html

Fedora Core 21

mediawiki-1.24.4-1.fc21

189927 - Fedora Linux 23 FEDORA-2015-2e7c06c639 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5161, CVE-2015-5723

Description

The scan detected that the host is missing the following update:
FEDORA-2015-2e7c06c639

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171108.html

Fedora Core 23

php-ZendFramework-1.12.16-1.fc23

189930 - Fedora Linux 23 FEDORA-2015-ec6d598d3d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8001, CVE-2015-8002, CVE-2015-8003, CVE-2015-8004, CVE-2015-8005, CVE-2015-8006, CVE-2015-8007, CVE-2015-8008, CVE-2015-8009

Description

The scan detected that the host is missing the following update:
FEDORA-2015-ec6d598d3d

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170979.html

Fedora Core 23

mediawiki-1.25.3-1.fc23

189931 - Fedora Linux 22 FEDORA-2015-6d70a701bf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5161, CVE-2015-5723

Description

The scan detected that the host is missing the following update:
FEDORA-2015-6d70a701bf

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171113.html

Fedora Core 22

php-ZendFramework-1.12.16-1.fc22

189935 - Fedora Linux 22 FEDORA-2015-24fe8b66c9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8001, CVE-2015-8002, CVE-2015-8003, CVE-2015-8004, CVE-2015-8005, CVE-2015-8006, CVE-2015-8007, CVE-2015-8008, CVE-2015-8009

Description

The scan detected that the host is missing the following update:
FEDORA-2015-24fe8b66c9

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171007.html

Fedora Core 22

mediawiki-1.25.3-1.fc22

19284 - Update for Windows Hyper-V to Address CPU Weakness (3108638)

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-8104

Description

Multiple denial of service vulnerabilities are present in some versions of Microsoft Windows.

Observation

Microsoft Windows is an industrial standard operating system.

Multiple denial of service vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in CPU but Microsoft's update provides protection in Hyper-V. Successful exploitation could allow an attacker to cause denial of service.

130313 - Debian Linux 7.0, 8.0 DSA-3392-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0852

Description

The scan detected that the host is missing the following update:
DSA-3392-1

Observation

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

http://www.debian.org/security/2015/dsa-3392

Debian 8.0
all
libfreeimage3_3.15.4-4.2
libfreeimage3-dbg_3.15.4-4.2
libfreeimage-dev_3.15.4-4.2

Debian 7.0
all
libfreeimage3_3.15.1-1.1

libfreeimage-dev_3.15.1-1.1
libfreeimage3-dbg_3.15.1-1.1

144033 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1929-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7873

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1929-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00044.html

SuSE Linux 13.1
noarch
phpMyAdmin-4.4.15.1-37.1

SuSE Linux 13.2
noarch
phpMyAdmin-4.4.15.1-17.1

144038 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1911-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7940

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1911-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00036.html

SuSE Linux 13.1
noarch
bouncycastle-1.53-8.3.1
bouncycastle-javadoc-1.53-8.3.1

SuSE Linux 13.2
noarch
bouncycastle-1.53-13.3.1
bouncycastle-javadoc-1.53-13.3.1

144044 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1909-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7437

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1909-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00034.html

SuSE Linux 13.1
x86_64
potrace-debuginfo-1.13-2.7.1
potrace-1.13-2.7.1
libpotrace0-1.13-2.7.1
libpotrace0-debuginfo-1.13-2.7.1
potrace-devel-1.13-2.7.1
potrace-debugsource-1.13-2.7.1

i586
potrace-debuginfo-1.13-2.7.1
potrace-1.13-2.7.1
libpotrace0-1.13-2.7.1
libpotrace0-debuginfo-1.13-2.7.1
potrace-devel-1.13-2.7.1
potrace-debugsource-1.13-2.7.1

SuSE Linux 13.2
x86_64
potrace-devel-1.13-4.7.1
libpotrace0-debuginfo-1.13-4.7.1
potrace-debuginfo-1.13-4.7.1
potrace-debugsource-1.13-4.7.1
libpotrace0-1.13-4.7.1
potrace-1.13-4.7.1

i586
potrace-devel-1.13-4.7.1
libpotrace0-debuginfo-1.13-4.7.1
potrace-debuginfo-1.13-4.7.1
potrace-debugsource-1.13-4.7.1
libpotrace0-1.13-4.7.1
potrace-1.13-4.7.1

189924 - Fedora Linux 23 FEDORA-2015-36b145bd37 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7236

Description

The scan detected that the host is missing the following update:
FEDORA-2015-36b145bd37

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171030.html

Fedora Core 23

rpcbind-0.2.3-0.4.fc23

189936 - Fedora Linux 23 FEDORA-2015-287c164df5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7873

Description

The scan detected that the host is missing the following update:
FEDORA-2015-287c164df5

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171310.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171311.html

Fedora Core 23

phpMyAdmin-4.5.1-1.fc23
php-udan11-sql-parser-3.0.4-1.fc23

189946 - Fedora Linux 21 FEDORA-2015-5c06260c4b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7873

Description

The scan detected that the host is missing the following update:
FEDORA-2015-5c06260c4b

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171327.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171326.html

Fedora Core 21

php-udan11-sql-parser-3.0.4-1.fc21
phpMyAdmin-4.5.1-1.fc21

130309 - Debian Linux 7.0, 8.0 DSA-3396-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5307, CVE-2015-7833, CVE-2015-7872, CVE-2015-7990

Description

The scan detected that the host is missing the following update:
DSA-3396-1

Observation

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

http://www.debian.org/security/2015/dsa-3396

Debian 8.0
all
scsi-core-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
fuse-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
mouse-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
fat-modules-3.16.0-4-armmp-di_3.16.7-ckt11-1+deb8u6
linux-headers-3.16.0-4-all-amd64_3.16.7-ckt11-1+deb8u6
usb-serial-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
usb-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
scsi-common-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
sata-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
xfs-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt11-1+deb8u6
usb-storage-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
mmc-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
nic-shared-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
usb-storage-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
nbd-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt11-1+deb8u6
squashfs-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
fat-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt11-1+deb8u6
linux-headers-3.16.0-4-powerpc_3.16.7-ckt11-1+deb8u6
udf-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
cdrom-core-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
usb-serial-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
jfs-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt11-1+deb8u6
pata-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
squashfs-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
crc-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
ext4-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
fb-modules-3.16.0-4-armmp-di_3.16.7-ckt11-1+deb8u6
sata-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
pcmcia-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt11-1+deb8u6
usb-storage-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
linux-headers-3.16.0-4-all-powerpc_3.16.7-ckt11-1+deb8u6
linux-image-3.16.0-4-loongson-2e_3.16.7-ckt11-1+deb8u6
crypto-dm-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
event-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
nic-wireless-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
fat-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
jfs-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
nic-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt11-1+deb8u6

sound-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
scsi-common-modules-3.16.0-4-versatile-di_3.16.7-ckt11-1+deb8u6
nic-pcmcia-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
md-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
scsi-extra-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
input-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
kernel-image-3.16.0-4-arm64-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
kernel-image-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
scsi-common-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
usb-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
ext4-modules-3.16.0-4-s390x-di_3.16.7-ckt11-1+deb8u6
cdrom-core-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
leds-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
jfs-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
linux-headers-3.16.0-4-s390x_3.16.7-ckt11-1+deb8u6
mmc-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
btrfs-modules-3.16.0-4-arm64-di_3.16.7-ckt11-1+deb8u6
nic-shared-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
core-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-armmp-di_3.16.7-ckt11-1+deb8u6
affs-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt11-1+deb8u6
ppp-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
nic-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
fat-modules-3.16.0-4-orion5x-di_3.16.7-ckt11-1+deb8u6
nbd-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
nic-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
md-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt11-1+deb8u6
fuse-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
pata-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
crypto-dm-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
scsi-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
mouse-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
jfs-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
nic-shared-modules-3.16.0-4-orion5x-di_3.16.7-ckt11-1+deb8u6
fuse-modules-3.16.0-4-versatile-di_3.16.7-ckt11-1+deb8u6
linux-image-3.16.0-4-5kc-malta_3.16.7-ckt11-1+deb8u6
squashfs-modules-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
usb-modules-3.16.0-4-armmp-di_3.16.7-ckt11-1+deb8u6
isofs-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
multipath-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
usb-serial-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
crypto-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt11-1+deb8u6
udf-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
btrfs-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
virtio-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt11-1+deb8u6
xfs-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
pcmcia-storage-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
kernel-image-3.16.0-4-kirkwood-di_3.16.7-ckt11-1+deb8u6
linux-manual-3.16_3.16.7-ckt11-1+deb8u6
btrfs-modules-3.16.0-4-versatile-di_3.16.7-ckt11-1+deb8u6
ppp-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
btrfs-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt11-1+deb8u6
zlib-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt11-1+deb8u6
jfs-modules-3.16.0-4-r5k-ip32-di_3.16.7-ckt11-1+deb8u6
sata-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
nic-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6
event-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt11-1+deb8u6
isofs-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
xfs-modules-3.16.0-4-octeon-di_3.16.7-ckt11-1+deb8u6

scsi-core-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt11-1+deb8u6
virtio-modules-3.16.0-4-loongson-2f-di_3.16.7-ckt11-1+deb8u6
zlib-modules-3.16.0-4-sb1-bcm91250a-di_3.16.7-ckt11-1+deb8u6
btrfs-modules-3.16.0-4-r4k-ip22-di_3.16.7-ckt11-1+deb8u6
squashfs-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
udf-modules-3.16.0-4-orion5x-di_3.16.7-ckt11-1+deb8u6
kernel-image-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
input-modules-3.16.0-4-loongson-3-di_3.16.7-ckt11-1+deb8u6
scsi-common-modules-3.16.0-4-686-pae-di_3.16.7-ckt11-1+deb8u6
event-modules-3.16.0-4-powerpc64-di_3.16.7-ckt11-1+deb8u6
usb-storage-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
ppp-modules-3.16.0-4-armmp-di_3.16.7-ckt11-1+deb8u6
hfs-modules-3.16.0-4-loongson-2e-di_3.16.7-ckt11-1+deb8u6
sound-modules-3.16.0-4-586-di_3.16.7-ckt11-1+deb8u6
mouse-modules-3.16.0-4-powerpc64le-di_3.16.7-ckt11-1+deb8u6
minix-modules-3.16.0-4-4kc-malta-di_3.16.7-ckt11-1+deb8u6
mmc-core-modules-3.16.0-4-amd64-di_3.16.7-ckt11-1+deb8u6
linux-doc-3.16_3.16.7-ckt11-1+deb8u6
nbd-modules-3.16.0-4-powerpc-di_3.16.7-ckt11-1+deb8u6
linux-image-3.16.0-4-arm64-dbg_3.16.7-ckt11-1+deb8u6

Debian 7.0
all
ata-modules-3.2.0-4-powerpc-di_3.2.68-1+deb7u6

140968 - Red Hat Enterprise Linux RHSA-2015-1979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3240

Description

The scan detected that the host is missing the following update:
RHSA-2015-1979

Observation

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

https://rhn.redhat.com/errata/RHSA-2015-1979.html

RHEL7D
x86_64
libreswan-3.15-5.el7_1
libreswan-debuginfo-3.15-5.el7_1

RHEL7S
x86_64
libreswan-3.15-5.el7_1
libreswan-debuginfo-3.15-5.el7_1

RHEL7WS
x86_64
libreswan-3.15-5.el7_1
libreswan-debuginfo-3.15-5.el7_1

185038 - Ubuntu Linux 14.04 USN-2797-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2925, CVE-2015-5257, CVE-2015-5283

Description

The scan detected that the host is missing the following update:
USN-2797-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003179.html

Ubuntu 14.04

linux-image-3.16.0-52-powerpc-e500mc_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-powerpc64-smp_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-lowlatency_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-powerpc64-emb_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-generic_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-generic-lpae_3.16.0-52.71~14.04.1
linux-image-3.16.0-52-powerpc-smp_3.16.0-52.71~14.04.1

88718 - Slackware Linux 14.1 SSA:2015-310-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2015-310-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.355602

Slackware 14.1
x86_64
mozilla-firefox-38.4.0esr-x86_64-1

130310 - Debian Linux 8.0 DSA-3391-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-3391-1

Observation

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

http://www.debian.org/security/2015/dsa-3391

Debian 8.0
all
php-horde_5.2.1+debian0-2+deb8u2

130311 - Debian Linux 7.0, 8.0 DSA-3394-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
DSA-3394-1

Observation

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

http://www.debian.org/security/2015/dsa-3394

Debian 8.0
all
libreoffice_1:4.3.3-2+deb8u2

Debian 7.0
all
libreoffice_1:3.5.4+dfsg2-0+deb7u5

144026 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1903-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7747

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1903-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00029.html

SuSE Linux 13.1
x86_64
audiofile-debugsource-0.3.6-2.3.1
audiofile-debuginfo-0.3.6-2.3.1
audiofile-devel-32bit-0.3.6-2.3.1

audiofile-0.3.6-2.3.1
libaudiofile1-debuginfo-32bit-0.3.6-2.3.1
libaudiofile1-0.3.6-2.3.1
libaudiofile1-debuginfo-0.3.6-2.3.1
libaudiofile1-32bit-0.3.6-2.3.1
audiofile-doc-0.3.6-2.3.1
audiofile-devel-0.3.6-2.3.1

i586
audiofile-debugsource-0.3.6-2.3.1
audiofile-debuginfo-0.3.6-2.3.1
audiofile-0.3.6-2.3.1
libaudiofile1-0.3.6-2.3.1
libaudiofile1-debuginfo-0.3.6-2.3.1
audiofile-doc-0.3.6-2.3.1
audiofile-devel-0.3.6-2.3.1

SuSE Linux 13.2
x86_64
libaudiofile1-debuginfo-32bit-0.3.6-6.3.1
audiofile-doc-0.3.6-6.3.1
audiofile-debugsource-0.3.6-6.3.1
audiofile-debuginfo-0.3.6-6.3.1
audiofile-devel-32bit-0.3.6-6.3.1
audiofile-0.3.6-6.3.1
audiofile-devel-0.3.6-6.3.1
libaudiofile1-debuginfo-0.3.6-6.3.1
libaudiofile1-0.3.6-6.3.1
libaudiofile1-32bit-0.3.6-6.3.1

i586
audiofile-doc-0.3.6-6.3.1
audiofile-debugsource-0.3.6-6.3.1
audiofile-debuginfo-0.3.6-6.3.1
audiofile-0.3.6-6.3.1
audiofile-devel-0.3.6-6.3.1
libaudiofile1-debuginfo-0.3.6-6.3.1
libaudiofile1-0.3.6-6.3.1

181662 - FreeBSD OpenOffice 4.1.1 Multiple Vulnerabilities (18b3c61b-83de-11e5-905b-ac9e174be3af)

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

Risk Level: Low

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
OpenOffice 4.1.1 -- multiple vulnerabilities (18b3c61b-83de-11e5-905b-ac9e174be3af)

Observation

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

http://www.vuxml.org/freebsd/18b3c61b-83de-11e5-905b-ac9e174be3af.html

Affected packages:
apache-openoffice < 4.1.2
apache-openoffice-devel < 4.2.1705368,3

181663 - FreeBSD PuTTY Memory Corruption In Terminal Emulator's Erase Character Handling (0cb0afd9-86b8-11e5-bf60-080027ef73ec)

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

Risk Level: Low

CVE: CVE-2015-5309

Description

The scan detected that the host is missing the following update:
PuTTY -- memory corruption in terminal emulator's erase character handling (0cb0afd9-86b8-11e5-bf60-080027ef73ec)

Observation

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

http://www.vuxml.org/freebsd/0cb0afd9-86b8-11e5-bf60-080027ef73ec.html

Affected packages:
0.54 <= putty < 0.66

181664 - FreeBSD powerdns Denial Of Service (56665ccb-8723-11e5-9b13-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-5311

Description

The scan detected that the host is missing the following update:
powerdns -- Denial of Service (56665ccb-8723-11e5-9b13-14dae9d210b8)

Observation

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

http://www.vuxml.org/freebsd/56665ccb-8723-11e5-9b13-14dae9d210b8.html

Affected packages:
3.4.4 <= powerdns < 3.4.7

185034 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2808-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5310, CVE-2015-5314, CVE-2015-5315, CVE-2015-5316

Description

The scan detected that the host is missing the following update:
USN-2808-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003189.html

Ubuntu 15.04

hostapd_2.1-0ubuntu7.3
wpasupplicant_2.1-0ubuntu7.3

Ubuntu 15.10

wpasupplicant_2.4-0ubuntu3.2
hostapd_2.4-0ubuntu3.2

Ubuntu 14.04

hostapd_2.1-0ubuntu1.4
wpasupplicant_2.1-0ubuntu1.4

185035 - Ubuntu Linux 14.04 USN-2805-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2805-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003186.html

Ubuntu 14.04

linux-image-3.16.0-53-powerpc64-smp_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-powerpc-e500mc_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-powerpc64-emb_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-powerpc-smp_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-generic_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-generic-lpae_3.16.0-53.72~14.04.1
linux-image-3.16.0-53-lowlatency_3.16.0-53.72~14.04.1

185037 - Ubuntu Linux 14.04 USN-2798-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2925, CVE-2015-5257

Description

The scan detected that the host is missing the following update:
USN-2798-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003178.html

Ubuntu 14.04

linux-image-3.19.0-32-lowlatency_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-powerpc64-emb_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-generic_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-generic-lpae_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-powerpc-smp_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-powerpc-e500mc_3.19.0-32.37~14.04.1
linux-image-3.19.0-32-powerpc64-smp_3.19.0-32.37~14.04.1

185039 - Ubuntu Linux 15.04 USN-2802-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2802-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003184.html

Ubuntu 15.04

linux-image-3.19.0-33-powerpc64-emb_3.19.0-33.38
linux-image-3.19.0-33-powerpc-smp_3.19.0-33.38
linux-image-3.19.0-33-powerpc64-smp_3.19.0-33.38
linux-image-3.19.0-33-generic_3.19.0-33.38
linux-image-3.19.0-33-lowlatency_3.19.0-33.38
linux-image-3.19.0-33-generic-lpae_3.19.0-33.38
linux-image-3.19.0-33-powerpc-e500mc_3.19.0-33.38

185042 - Ubuntu Linux 15.10 USN-2803-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2803-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003185.html

Ubuntu 15.10

linux-image-4.2.0-18-powerpc-e500mc_4.2.0-18.22
linux-image-4.2.0-18-generic_4.2.0-18.22
linux-image-4.2.0-18-powerpc64-smp_4.2.0-18.22
linux-image-4.2.0-18-powerpc-smp_4.2.0-18.22
linux-image-4.2.0-18-lowlatency_4.2.0-18.22
linux-image-4.2.0-18-powerpc64-emb_4.2.0-18.22
linux-image-4.2.0-18-generic-lpae_4.2.0-18.22

185043 - Ubuntu Linux 12.04 USN-2800-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2800-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003182.html

Ubuntu 12.04

linux-image-3.2.0-94-highbank_3.2.0-94.134
linux-image-3.2.0-94-generic_3.2.0-94.134
linux-image-3.2.0-94-powerpc64-smp_3.2.0-94.134
linux-image-3.2.0-94-powerpc-smp_3.2.0-94.134
linux-image-3.2.0-94-generic-pae_3.2.0-94.134
linux-image-3.2.0-94-virtual_3.2.0-94.134
linux-image-3.2.0-94-omap_3.2.0-94.134

185044 - Ubuntu Linux 14.04 USN-2794-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2925, CVE-2015-5257

Description

The scan detected that the host is missing the following update:
USN-2794-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003175.html

Ubuntu 14.04

linux-image-3.13.0-67-generic-lpae_3.13.0-67.110
linux-image-3.13.0-67-generic_3.13.0-67.110
linux-image-3.13.0-67-powerpc-e500mc_3.13.0-67.110

linux-image-3.13.0-67-powerpc64-smp_3.13.0-67.110
linux-image-3.13.0-67-powerpc-e500_3.13.0-67.110
linux-image-3.13.0-67-powerpc64-emb_3.13.0-67.110
linux-image-3.13.0-67-lowlatency_3.13.0-67.110
linux-image-3.13.0-67-powerpc-smp_3.13.0-67.110

185045 - Ubuntu Linux 12.04 USN-2795-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2925, CVE-2015-5257

Description

The scan detected that the host is missing the following update:
USN-2795-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003176.html

Ubuntu 12.04

linux-image-3.13.0-67-generic_3.13.0-67.110~precise1
linux-image-3.13.0-67-generic-lpae_3.13.0-67.110~precise1

185046 - Ubuntu Linux 12.04, 14.04, 15.04 USN-2793-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-4551, CVE-2015-5212, CVE-2015-5213, CVE-2015-5214

Description

The scan detected that the host is missing the following update:
USN-2793-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003173.html

Ubuntu 12.04

libreoffice-core_3.5.7-0ubuntu9

Ubuntu 15.04

libreoffice-core_4.4.6~rc3-0ubuntu1

Ubuntu 14.04

libreoffice-core_4.2.8-0ubuntu3

185048 - Ubuntu Linux 15.04 USN-2799-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2925, CVE-2015-5257

Description

The scan detected that the host is missing the following update:
USN-2799-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003180.html

Ubuntu 15.04

linux-image-3.19.0-32-powerpc64-emb_3.19.0-32.37
linux-image-3.19.0-32-generic_3.19.0-32.37
linux-image-3.19.0-32-powerpc-e500mc_3.19.0-32.37
linux-image-3.19.0-32-generic-lpae_3.19.0-32.37
linux-image-3.19.0-32-powerpc64-smp_3.19.0-32.37
linux-image-3.19.0-32-powerpc-smp_3.19.0-32.37
linux-image-3.19.0-32-lowlatency_3.19.0-32.37

185049 - Ubuntu Linux 14.04 USN-2806-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2806-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003188.html

Ubuntu 14.04

linux-image-3.19.0-33-powerpc-e500mc_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-powerpc64-smp_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-generic_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-generic-lpae_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-powerpc-smp_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-powerpc64-emb_3.19.0-33.38~14.04.1
linux-image-3.19.0-33-lowlatency_3.19.0-33.38~14.04.1

185050 - Ubuntu Linux 14.04 USN-2807-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2807-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003190.html

Ubuntu 14.04

linux-image-4.2.0-18-powerpc-smp_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-generic-lpae_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-powerpc-e500mc_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-powerpc64-smp_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-powerpc64-emb_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-lowlatency_4.2.0-18.22~14.04.1
linux-image-4.2.0-18-generic_4.2.0-18.22~14.04.1

185051 - Ubuntu Linux 12.04 USN-2804-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2804-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003187.html

Ubuntu 12.04

linux-image-3.13.0-68-generic-lpae_3.13.0-68.111~precise1
linux-image-3.13.0-68-generic_3.13.0-68.111~precise1

185053 - Ubuntu Linux 14.04 USN-2801-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5307

Description

The scan detected that the host is missing the following update:
USN-2801-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003183.html

Ubuntu 14.04

linux-image-3.13.0-68-powerpc-e500mc_3.13.0-68.111
linux-image-3.13.0-68-lowlatency_3.13.0-68.111
linux-image-3.13.0-68-powerpc64-emb_3.13.0-68.111
linux-image-3.13.0-68-powerpc-e500_3.13.0-68.111
linux-image-3.13.0-68-powerpc64-smp_3.13.0-68.111
linux-image-3.13.0-68-generic-lpae_3.13.0-68.111
linux-image-3.13.0-68-generic_3.13.0-68.111
linux-image-3.13.0-68-powerpc-smp_3.13.0-68.111

189917 - Fedora Linux 21 FEDORA-2015-a381facfd9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a381facfd9

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170933.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170931.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170932.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170934.html

Fedora Core 21

php-horde-passwd-5.0.4-1.fc21
php-horde-ingo-3.2.7-1.fc21
php-horde-horde-5.2.8-1.fc21
php-horde-imp-6.2.11-1.fc21

189918 - Fedora Linux 22 FEDORA-2015-31284f029f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-31284f029f

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170873.html

Fedora Core 22

libsbw-2.11.1-9.20150414svn579.fc22

189923 - Fedora Linux 22 FEDORA-2015-cf767c77c1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-cf767c77c1

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171055.html

Fedora Core 22

git-2.4.3-7.fc22

189925 - Fedora Linux 22 FEDORA-2015-0d0df8d770 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-0d0df8d770

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171001.html

Fedora Core 22

xscreensaver-5.34-1.fc22

189926 - Fedora Linux 22 FEDORA-2015-37090f89d8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

FEDORA-2015-37090f89d8

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170887.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170888.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170886.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170885.html

Fedora Core 22

php-horde-ingo-3.2.7-1.fc22
php-horde-imp-6.2.11-1.fc22
php-horde-passwd-5.0.4-1.fc22
php-horde-horde-5.2.8-1.fc22

189928 - Fedora Linux 22 FEDORA-2015-5b5109510c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-5b5109510c

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170860.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170862.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170861.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170863.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170864.html

Fedora Core 22

nss-3.20.1-1.0.fc22
nss-util-3.20.1-1.0.fc22
nspr-4.10.10-1.fc22
firefox-42.0-2.fc22
nss-softokn-3.20.1-1.0.fc22

189929 - Fedora Linux 23 FEDORA-2015-2880ac7065 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-2880ac7065

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170731.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170728.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170730.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170732.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170729.html

Fedora Core 23

nss-util-3.20.1-1.0.fc23
nss-softokn-3.20.1-1.0.fc23
nss-3.20.1-1.0.fc23
nspr-4.10.10-1.fc23
firefox-42.0-2.fc23

189932 - Fedora Linux 22 FEDORA-2015-20a20a4129 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-20a20a4129

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170877.html

Fedora Core 22

seqan-1.4.2-21.fc22

189933 - Fedora Linux 23 FEDORA-2015-386863df8a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5602

Description

The scan detected that the host is missing the following update:
FEDORA-2015-386863df8a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171024.html

Fedora Core 23

sudo-1.8.15-1.fc23

189934 - Fedora Linux 22 FEDORA-2015-bbb6a72996 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-bbb6a72996

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171183.html

Fedora Core 22

icecat-38.3.0-10.fc22

189937 - Fedora Linux 23 FEDORA-2015-15291 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5215, CVE-2015-5216, CVE-2015-5217, CVE-2015-5301

Description

The scan detected that the host is missing the following update:
FEDORA-2015-15291

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171052.html

Fedora Core 23

ipsilon-1.1.1-2.fc23

189938 - Fedora Linux 21 FEDORA-2015-15290 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5301

Description

The scan detected that the host is missing the following update:
FEDORA-2015-15290

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171076.html

Fedora Core 21

ipsilon-1.1.1-2.fc21

189939 - Fedora Linux 22 FEDORA-2015-15292 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5215, CVE-2015-5216, CVE-2015-5217, CVE-2015-5301

Description

The scan detected that the host is missing the following update:
FEDORA-2015-15292

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171067.html

Fedora Core 22

ipsilon-1.1.1-2.fc22

189940 - Fedora Linux 23 FEDORA-2015-85bfa4ba56 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-85bfa4ba56

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171128.html

Fedora Core 23

icecat-38.3.0-10.fc23

189941 - Fedora Linux 21 FEDORA-2015-adfd729dbc Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-adfd729dbc

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170958.html

Fedora Core 21

xscreensaver-5.34-1.fc21

189942 - Fedora Linux 21 FEDORA-2015-77bfbc1bcd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7852, CVE-2015-7871

Description

The scan detected that the host is missing the following update:
FEDORA-2015-77bfbc1bcd

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170926.html

Fedora Core 21

ntp-4.2.6p5-34.fc21

189943 - Fedora Linux 21 FEDORA-2015-fb3360fc0a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-fb3360fc0a

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171239.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171243.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171240.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171241.html
http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171242.html

Fedora Core 21

nspr-4.10.10-1.fc21
firefox-42.0-2.fc21
nss-util-3.20.1-1.0.fc21
nss-3.20.1-1.0.fc21
nss-softokn-3.20.1-1.0.fc21

189944 - Fedora Linux 23 FEDORA-2015-a26f0b0daf Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-a26f0b0daf

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170967.html

Fedora Core 23

python-pycurl-7.19.5.1-4.fc23

189945 - Fedora Linux 22 FEDORA-2015-6a267387c0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5602

Description

The scan detected that the host is missing the following update:
FEDORA-2015-6a267387c0

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171054.html

Fedora Core 22

sudo-1.8.15-1.fc22

189948 - Fedora Linux 23 FEDORA-2015-58ae075703 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2698

Description

The scan detected that the host is missing the following update:
FEDORA-2015-58ae075703

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171079.html

Fedora Core 23

krb5-1.13.2-13.fc23

189949 - Fedora Linux 21 FEDORA-2015-d0e48b2eb1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d0e48b2eb1

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171244.html

Fedora Core 21

icecat-38.3.0-10.fc21

189950 - Fedora Linux 22 FEDORA-2015-cb94fd13d8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7943

Description

The scan detected that the host is missing the following update:
FEDORA-2015-cb94fd13d8

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/171006.html

Fedora Core 22

drupal7-7.41-1.fc22

189951 - Fedora Linux 21 FEDORA-2015-9e842ac36e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2015-9e842ac36e

Observation

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

http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170927.html

Fedora Core 21

seqan-1.4.2-21.fc21

144039 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1910-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5218

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1910-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2015-11/msg00035.html

SuSE Linux 13.1
i586
libblkid-devel-2.23.2-34.1
libuuid1-2.23.2-34.1
libmount1-2.23.2-34.1
libuuid1-debuginfo-2.23.2-34.1
libblkid1-2.23.2-34.1
util-linux-debuginfo-2.23.2-34.1
libmount-devel-2.23.2-34.1
util-linux-debugsource-2.23.2-34.1
libuuid-devel-2.23.2-34.1
util-linux-2.23.2-34.1
uuidd-debuginfo-2.23.2-34.1
libblkid1-debuginfo-2.23.2-34.1
uuidd-2.23.2-34.1
libmount1-debuginfo-2.23.2-34.1

noarch
util-linux-lang-2.23.2-34.1

x86_64
libuuid-devel-32bit-2.23.2-34.1
libmount-devel-32bit-2.23.2-34.1
libmount1-debuginfo-32bit-2.23.2-34.1
libblkid-devel-2.23.2-34.1
libuuid1-2.23.2-34.1
libmount1-2.23.2-34.1
libuuid1-debuginfo-2.23.2-34.1
libblkid1-2.23.2-34.1
util-linux-debuginfo-2.23.2-34.1
libmount-devel-2.23.2-34.1
libuuid1-32bit-2.23.2-34.1
util-linux-debugsource-2.23.2-34.1
libblkid1-32bit-2.23.2-34.1
libuuid-devel-2.23.2-34.1
libblkid1-debuginfo-32bit-2.23.2-34.1
libblkid-devel-32bit-2.23.2-34.1
util-linux-2.23.2-34.1
uuidd-debuginfo-2.23.2-34.1
libblkid1-debuginfo-2.23.2-34.1
uuidd-2.23.2-34.1
libmount1-32bit-2.23.2-34.1
libmount1-debuginfo-2.23.2-34.1
libuuid1-debuginfo-32bit-2.23.2-34.1

SuSE Linux 13.2
i586
libmount-devel-static-2.25.1-20.1
uuidd-2.25.1-20.1
util-linux-systemd-debugsource-2.25.1-20.1
libblkid1-2.25.1-20.1
libblkid-devel-static-2.25.1-20.1
libuuid-devel-static-2.25.1-20.1
libsmartcols1-2.25.1-20.1
libblkid1-debuginfo-2.25.1-20.1
util-linux-debugsource-2.25.1-20.1
libsmartcols-devel-static-2.25.1-20.1
libmount1-debuginfo-2.25.1-20.1
python-libmount-2.25.1-20.2
uuidd-debuginfo-2.25.1-20.1
libmount-devel-2.25.1-20.1
libblkid-devel-2.25.1-20.1
libuuid1-debuginfo-2.25.1-20.1
util-linux-2.25.1-20.1
libsmartcols1-debuginfo-2.25.1-20.1
libsmartcols-devel-2.25.1-20.1
libuuid-devel-2.25.1-20.1
libmount1-2.25.1-20.1
util-linux-systemd-2.25.1-20.1
libuuid1-2.25.1-20.1
util-linux-debuginfo-2.25.1-20.1
util-linux-systemd-debuginfo-2.25.1-20.1
python-libmount-debuginfo-2.25.1-20.2
python-libmount-debugsource-2.25.1-20.2

noarch
util-linux-lang-2.25.1-20.1

x86_64
libmount-devel-static-2.25.1-20.1

libuuid1-debuginfo-32bit-2.25.1-20.1
uuidd-2.25.1-20.1
util-linux-systemd-debugsource-2.25.1-20.1
libblkid1-debuginfo-32bit-2.25.1-20.1
libblkid1-2.25.1-20.1
libblkid-devel-static-2.25.1-20.1
libuuid-devel-static-2.25.1-20.1
libmount1-32bit-2.25.1-20.1
libsmartcols1-2.25.1-20.1
libblkid1-debuginfo-2.25.1-20.1
libmount-devel-32bit-2.25.1-20.1
util-linux-debugsource-2.25.1-20.1
libsmartcols-devel-static-2.25.1-20.1
libmount1-debuginfo-2.25.1-20.1
python-libmount-2.25.1-20.2
uuidd-debuginfo-2.25.1-20.1
libmount-devel-2.25.1-20.1
libblkid-devel-2.25.1-20.1
libblkid1-32bit-2.25.1-20.1
libuuid1-debuginfo-2.25.1-20.1
util-linux-2.25.1-20.1
libsmartcols1-debuginfo-2.25.1-20.1
libsmartcols-devel-2.25.1-20.1
libuuid-devel-2.25.1-20.1
libmount1-2.25.1-20.1
libuuid1-32bit-2.25.1-20.1
util-linux-systemd-2.25.1-20.1
libuuid1-2.25.1-20.1
libblkid-devel-32bit-2.25.1-20.1
util-linux-debuginfo-2.25.1-20.1
libuuid-devel-32bit-2.25.1-20.1
libmount1-debuginfo-32bit-2.25.1-20.1
util-linux-systemd-debuginfo-2.25.1-20.1
python-libmount-debuginfo-2.25.1-20.2
python-libmount-debugsource-2.25.1-20.2

ENHANCED CHECKS

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

181512 - FreeBSD wpa_supplicant WPS_NFC Option Payload Length Validation Vulnerability (c93c9395-25e1-11e5-a4a5-002590263bf5)

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

Risk Level: Low

CVE: CVE-2015-8041

Update Details

CVE is updated

181647 - FreeBSD lldpd Buffer Overflow (2a4a112a-7c1b-11e5-bd77-0800275369e2)

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

Risk Level: Low

CVE: CVE-2015-8011, CVE-2015-8012

Update Details

CVE is updated FASLScript is updated

181652 - FreeBSD Xscreensaver - Lock Bypass (4b9393b8-7c0c-11e5-a010-080027ddead3)

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

Risk Level: Low

CVE: CVE-2015-8025

Update Details

CVE is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.