

MCAFFEE 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

88716 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-302-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3520, CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2014-8137, CVE-2014-8138, CVE-2014-8157, CVE-2014-8158, CVE-2014-9029

Description

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

SSA:2015-302-02

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.538606>

Slackware 14.0

x86_64

jasper-1.900.1-x86_64-4

Slackware 13.0

x86_64

jasper-1.900.1-x86_64-3

Slackware 13.1

x86_64

jasper-1.900.1-x86_64-4

Slackware 14.1

x86_64

jasper-1.900.1-x86_64-4

Slackware 13.37

x86_64

jasper-1.900.1-x86_64-4

130301 - Debian Linux 7.0, 8.0 DSA-3381-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian 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:

DSA-3381-1

Observation

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

For more information see:

<http://www.debian.org/security/2015/dsa-3381>

Debian 8.0

all

openjdk-7-jdk_7u85-2.6.1-5~deb8u1
openjdk-7-jre-zero_7u85-2.6.1-5~deb8u1
openjdk-7-demo_7u85-2.6.1-5~deb8u1
openjdk-7-source_7u85-2.6.1-5~deb8u1
openjdk-7-jre-headless_7u85-2.6.1-5~deb8u1
icedtea-7-jre-jamvm_7u85-2.6.1-5~deb8u1
openjdk-7-jre-lib_7u85-2.6.1-5~deb8u1
openjdk-7-jre_7u85-2.6.1-5~deb8u1
openjdk-7-doc_7u85-2.6.1-5~deb8u1
openjdk-7-dbg_7u85-2.6.1-5~deb8u1

Debian 7.0

all

openjdk-7-jre-zero_7u85-2.6.1-6~deb7u1
icedtea-7-jre-cacao_7u85-2.6.1-6~deb7u1
openjdk-7-jre-lib_7u85-2.6.1-6~deb7u1
openjdk-7-demo_7u85-2.6.1-6~deb7u1
openjdk-7-jre_7u85-2.6.1-6~deb7u1
openjdk-7-doc_7u85-2.6.1-6~deb7u1
icedtea-7-jre-jamvm_7u85-2.6.1-6~deb7u1
openjdk-7-source_7u85-2.6.1-6~deb7u1
openjdk-7-jdk_7u85-2.6.1-6~deb7u1
openjdk-7-jre-headless_7u85-2.6.1-6~deb7u1
openjdk-7-dbg_7u85-2.6.1-6~deb7u1

144017 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1874-2 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:

SUSE-SU-2015:1874-2

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/001659.html>

SuSE SLED 12

x86_64

java-1_7_0-openjdk-debugsource-1.7.0.91-21.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-1.7.0.91-21.2
java-1_7_0-openjdk-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-headless-1.7.0.91-21.2

SuSE SLES 12

x86_64

java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-devel-1.7.0.91-21.2
java-1_7_0-openjdk-demo-1.7.0.91-21.2
java-1_7_0-openjdk-headless-1.7.0.91-21.2
java-1_7_0-openjdk-1.7.0.91-21.2
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-debugsource-1.7.0.91-21.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-21.2

144018 - SuSE SLES 12 SUSE-SU-2015:1874-1 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:

SUSE-SU-2015:1874-1

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/001655.html>

SuSE SLES 12

ppc64le

java-1_7_0-openjdk-demo-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-devel-1.7.0.91-21.2
java-1_7_0-openjdk-demo-1.7.0.91-21.2
java-1_7_0-openjdk-headless-1.7.0.91-21.2
java-1_7_0-openjdk-1.7.0.91-21.2
java-1_7_0-openjdk-devel-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-debuginfo-1.7.0.91-21.2
java-1_7_0-openjdk-debugsource-1.7.0.91-21.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.91-21.2

170581 - Amazon Linux AMI ALAS-2015-605 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4840, 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:
ALAS-2015-605

Observation

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

<https://alas.aws.amazon.com/ALAS-2015-605.html>

Amazon Linux AMI

i686

java-1.7.0-openjdk-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.2.63.amzn1

noarch

java-1.7.0-openjdk-javadoc-1.7.0.91-2.6.2.2.63.amzn1

x86_64

java-1.7.0-openjdk-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-demo-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-src-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-devel-1.7.0.91-2.6.2.2.63.amzn1
java-1.7.0-openjdk-debuginfo-1.7.0.91-2.6.2.2.63.amzn1

170582 - Amazon Linux AMI ALAS-2015-606 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
ALAS-2015-606

Observation

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

<https://alas.aws.amazon.com/ALAS-2015-606.html>

Amazon Linux AMI

i686

java-1.8.0-openjdk-headless-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-devel-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-src-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-demo-1.8.0.65-2.b17.7.amzn1

noarch

java-1.8.0-openjdk-javadoc-1.8.0.65-2.b17.7.amzn1

x86_64
java-1.8.0-openjdk-headless-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-debuginfo-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-devel-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-src-1.8.0.65-2.b17.7.amzn1
java-1.8.0-openjdk-demo-1.8.0.65-2.b17.7.amzn1

185030 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2784-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
USN-2784-1

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-October/003165.html>

Ubuntu 15.04

openjdk-7-jre-headless_7u85-2.6.1-5ubuntu0.15.04.1
icedtea-7-jre-jamvm_7u85-2.6.1-5ubuntu0.15.04.1
openjdk-7-jre-zero_7u85-2.6.1-5ubuntu0.15.04.1
openjdk-7-jre_7u85-2.6.1-5ubuntu0.15.04.1
openjdk-7-jre-lib_7u85-2.6.1-5ubuntu0.15.04.1

Ubuntu 15.10

openjdk-7-jre_7u85-2.6.1-5ubuntu0.15.10.1
openjdk-7-jre-headless_7u85-2.6.1-5ubuntu0.15.10.1
openjdk-7-jre-lib_7u85-2.6.1-5ubuntu0.15.10.1
openjdk-7-jre-zero_7u85-2.6.1-5ubuntu0.15.10.1
icedtea-7-jre-jamvm_7u85-2.6.1-5ubuntu0.15.10.1

Ubuntu 14.04

openjdk-7-jre-lib_7u85-2.6.1-5ubuntu0.14.04.1
openjdk-7-jre-headless_7u85-2.6.1-5ubuntu0.14.04.1
icedtea-7-jre-jamvm_7u85-2.6.1-5ubuntu0.14.04.1
openjdk-7-jre-zero_7u85-2.6.1-5ubuntu0.14.04.1
openjdk-7-jre_7u85-2.6.1-5ubuntu0.14.04.1

19180 - (HT205375) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2012-6151, CVE-2014-3565, CVE-2015-0235, CVE-2015-0273, CVE-2015-5924, CVE-2015-5925, CVE-2015-5926, CVE-2015-5927, CVE-2015-5932, CVE-2015-5933, CVE-2015-5934, CVE-2015-5935, CVE-2015-5936, CVE-2015-5937, CVE-2015-5938, CVE-2015-5939, CVE-2015-5940, CVE-2015-5942, CVE-2015-5943, CVE-2015-5944, CVE-2015-5945, CVE-2015-6563, CVE-2015-

6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838, CVE-2015-6974, CVE-2015-6975, CVE-2015-6976, CVE-2015-6977, CVE-2015-6978, CVE-2015-6983, CVE-2015-6984, CVE-2015-6985, CVE-2015-6987, CVE-2015-6988, CVE-2015-6989, CVE-2015-6990, CVE-2015-6991, CVE-2015-6992, CVE-2015-6993, CVE-2015-6994, CVE-2015-6995, CVE-2015-6996, CVE-2015-7003, CVE-2015-7006, CVE-2015-7007, CVE-2015-7008, CVE-2015-7009, CVE-2015-7010, CVE-2015-7015, CVE-2015-7016, CVE-2015-7017, CVE-2015-7018, CVE-2015-7019, CVE-2015-7020, CVE-2015-7021, CVE-2015-7023, CVE-2015-7035

Description

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

Observation

Apple OS X is the operating system used in Apple computers.

Multiple vulnerabilities are present in some versions of Apple OS X. The flaws lie in kernel and multiple other components. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service and execute arbitrary code.

19193 - Cisco Adaptive Security Appliance DNS Denial of Service I

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6325

Description

A vulnerability in some versions of Cisco Adaptive Security Appliance could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco Adaptive Security Appliance could lead to a denial of service.

The flaw is due to improper processing of DNS packets. Successful exploitation by a remote attacker could result in a denial of service condition.

170580 - Amazon Linux AMI ALAS-2015-604 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-0455, CVE-2007-2756, CVE-2007-3472, CVE-2007-3473, CVE-2009-3546, CVE-2015-0848, CVE-2015-4588, CVE-2015-4695, CVE-2015-4696

Description

The scan detected that the host is missing the following update:
ALAS-2015-604

Observation

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

<https://alas.aws.amazon.com/ALAS-2015-604.html>

Amazon Linux AMI

x86_64

libwmf-debuginfo-0.2.8.4-41.11.amzn1

libwmf-devel-0.2.8.4-41.11.amzn1

libwmf-lite-0.2.8.4-41.11.amzn1

libwmf-0.2.8.4-41.11.amzn1

i686

libwfmf-debuginfo-0.2.8.4-41.11.amzn1
libwfmf-devel-0.2.8.4-41.11.amzn1
libwfmf-lite-0.2.8.4-41.11.amzn1
libwfmf-0.2.8.4-41.11.amzn1

19196 - Cisco Adaptive Security Appliance DNS Denial of Service II

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6326

Description

A vulnerability in some versions of Cisco Adaptive Security Appliance could lead to a denial of service.

Observation

A vulnerability in some versions of Cisco Adaptive Security Appliance could lead to a denial of service.

The flaw is due to improper processing of DNS packets. Successful exploitation by a remote attacker could result in a denial of service condition.

88717 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-302-01 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SSA:2015-302-01

Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.513154>

Slackware 14.0
x86_64
curl-7.45.0-x86_64-1

Slackware 13.0
x86_64
curl-7.45.0-x86_64-1

Slackware 13.1
x86_64
curl-7.45.0-x86_64-1

Slackware 14.1
x86_64
curl-7.45.0-x86_64-1

Slackware 13.37
x86_64
curl-7.45.0-x86_64-1

130303 - Debian Linux 7.0, 8.0 DSA-3390-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7835

Description

The scan detected that the host is missing the following update:
DSA-3390-1

Observation

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

<http://www.debian.org/security/2015/dsa-3390>

Debian 8.0

all

xenstore-utils_4.4.1-9+deb8u2
xen-hypervisor-4.4-armhf_4.4.1-9+deb8u2
libxenstore3.0_4.4.1-9+deb8u2
xen-utils-common_4.4.1-9+deb8u2
xen-system-arm64_4.4.1-9+deb8u2
xen-system-armhf_4.4.1-9+deb8u2
xen-utils-4.4_4.4.1-9+deb8u2
xen-hypervisor-4.4-amd64_4.4.1-9+deb8u2
libxen-dev_4.4.1-9+deb8u2
xen-hypervisor-4.4-arm64_4.4.1-9+deb8u2
xen-system-amd64_4.4.1-9+deb8u2
libxen-4.4_4.4.1-9+deb8u2

Debian 7.0

all

xen-hypervisor-4.1-i386_4.1.4-3+deb7u9
xenstore-utils_4.1.4-3+deb7u9
xen-docs-4.1_4.1.4-3+deb7u9
libxenstore3.0_4.1.4-3+deb7u9
xen-utils-4.1_4.1.4-3+deb7u9
libxen-4.1_4.1.4-3+deb7u9
libxen-dev_4.1.4-3+deb7u9
xen-system-amd64_4.1.4-3+deb7u9
xen-system-i386_4.1.4-3+deb7u9
libxen-ocaml_4.1.4-3+deb7u9
xen-hypervisor-4.1-amd64_4.1.4-3+deb7u9
libxen-ocaml-dev_4.1.4-3+deb7u9
xen-utils-common_4.1.4-3+deb7u9

130304 - Debian Linux 8.0 DSA-3385-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4792, CVE-2015-4802, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4870, CVE-2015-4879, CVE-2015-4895, CVE-2015-4913

Description

The scan detected that the host is missing the following update:
DSA-3385-1

Observation

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

<http://www.debian.org/security/2015/dsa-3385>

Debian 8.0

all

mariadb-ocgraph-engine-10.0_10.0.22-0+deb8u1

mariadb-connect-engine-10.0_10.0.22-0+deb8u1

mariadb-test_10.0.22-0+deb8u1

mariadb-test-10.0_10.0.22-0+deb8u1

mariadb-client-10.0_10.0.22-0+deb8u1

mariadb-server-core-10.0_10.0.22-0+deb8u1

mariadb-server_10.0.22-0+deb8u1

mariadb-client-core-10.0_10.0.22-0+deb8u1

libmariadb-dev_10.0.22-0+deb8u1

mariadb-server-10.0_10.0.22-0+deb8u1

mariadb-common_10.0.22-0+deb8u1

mariadb-client_10.0.22-0+deb8u1

132194 - Oracle VM OVMSA-2015-0142 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2212, CVE-2014-8867, CVE-2015-7835, CVE-2015-7969, CVE-2015-7971

Description

The scan detected that the host is missing the following update:
OVMSA-2015-0142

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2015-October/000373.html>

OVM3.2

x86_64

xen-4.1.3-25.el5.127.79

xen-tools-4.1.3-25.el5.127.79

xen-devel-4.1.3-25.el5.127.79

132195 - Oracle VM OVMSA-2015-0141 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-2015-0141

Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2015-October/000374.html>

OVM3.3
x86_64
xen-4.3.0-55.el6.47.58
xen-tools-4.3.0-55.el6.47.58

144016 - SuSE Linux 13.2 openSUSE-SU-2015:1842-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0272, CVE-2015-1333, CVE-2015-2925, CVE-2015-3290, CVE-2015-5283, CVE-2015-5707, CVE-2015-7872

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1842-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-10/msg00056.html>

SuSE Linux 13.2
i586
kernel-default-debugsource-3.16.7-29.1
crash-devel-7.0.8-13.2
ipset-6.23-13.2
ipset-kmp-xen-6.23_k3.16.7_29-13.2
cloop-kmp-default-2.639_k3.16.7_29-14.13.2
cloop-debugsource-2.639-14.13.2
crash-kmp-desktop-debuginfo-7.0.8_k3.16.7_29-13.2
cloop-2.639-14.13.2
ipset-debugsource-6.23-13.2
kernel-default-devel-3.16.7-29.1
hdjmod-kmp-pae-debuginfo-1.28_k3.16.7_29-18.14.2
bbswitch-kmp-pae-0.8_k3.16.7_29-3.13.2
pcfclock-0.44-260.13.2
cloop-kmp-pae-debuginfo-2.639_k3.16.7_29-14.13.2
kernel-ec2-3.16.7-29.1
bbswitch-kmp-desktop-0.8_k3.16.7_29-3.13.2
hdjmod-kmp-default-debuginfo-1.28_k3.16.7_29-18.14.2
kernel-obs-qa-xen-3.16.7-29.1
pcfclock-kmp-default-debuginfo-0.44_k3.16.7_29-260.13.2
kernel-obs-build-3.16.7-29.2
xtables-addons-kmp-desktop-2.6_k3.16.7_29-13.2
bbswitch-kmp-desktop-debuginfo-0.8_k3.16.7_29-3.13.2
crash-debuginfo-7.0.8-13.2
xtables-addons-kmp-xen-debuginfo-2.6_k3.16.7_29-13.2
kernel-obs-qa-3.16.7-29.1
crash-eppic-debuginfo-7.0.8-13.2
cloop-kmp-default-debuginfo-2.639_k3.16.7_29-14.13.2
bbswitch-kmp-default-debuginfo-0.8_k3.16.7_29-3.13.2
xtables-addons-kmp-pae-2.6_k3.16.7_29-13.2
kernel-syms-3.16.7-29.1

pcfclock-kmp-desktop-debuginfo-0.44_k3.16.7_29-260.13.2
crash-eppic-7.0.8-13.2
kernel-ec2-base-3.16.7-29.1
crash-kmp-desktop-7.0.8_k3.16.7_29-13.2
crash-gcore-debuginfo-7.0.8-13.2
vhba-kmp-default-20140629_k3.16.7_29-2.13.2
xen-devel-4.4.2_06-27.2
bbswitch-0.8-3.13.2
hdjmod-kmp-xen-debuginfo-1.28_k3.16.7_29-18.14.2
pcfclock-debugsource-0.44-260.13.2
hdjmod-kmp-xen-1.28_k3.16.7_29-18.14.2
crash-kmp-pae-debuginfo-7.0.8_k3.16.7_29-13.2
pcfclock-kmp-pae-debuginfo-0.44_k3.16.7_29-260.13.2
crash-kmp-xen-debuginfo-7.0.8_k3.16.7_29-13.2
hdjmod-kmp-desktop-1.28_k3.16.7_29-18.14.2
pcfclock-kmp-pae-0.44_k3.16.7_29-260.13.2
crash-kmp-default-7.0.8_k3.16.7_29-13.2
xtables-addons-debuginfo-2.6-13.2
ipset-kmp-desktop-6.23_k3.16.7_29-13.2
kernel-ec2-devel-3.16.7-29.1
xtables-addons-kmp-default-2.6_k3.16.7_29-13.2
ipset-kmp-xen-debuginfo-6.23_k3.16.7_29-13.2
ipset-kmp-desktop-debuginfo-6.23_k3.16.7_29-13.2
libipset3-debuginfo-6.23-13.2
xen-libs-4.4.2_06-27.2
cloop-kmp-pae-2.639_k3.16.7_29-14.13.2
ipset-debuginfo-6.23-13.2
kernel-default-3.16.7-29.1
pcfclock-kmp-default-0.44_k3.16.7_29-260.13.2
ipset-kmp-default-debuginfo-6.23_k3.16.7_29-13.2
kernel-default-base-3.16.7-29.1
xtables-addons-kmp-default-debuginfo-2.6_k3.16.7_29-13.2
vhba-kmp-pae-20140629_k3.16.7_29-2.13.2
ipset-kmp-default-6.23_k3.16.7_29-13.2
xen-tools-domU-4.4.2_06-27.2
crash-7.0.8-13.2
hdjmod-kmp-default-1.28_k3.16.7_29-18.14.2
xen-libs-debuginfo-4.4.2_06-27.2
crash-debugsource-7.0.8-13.2
xtables-addons-kmp-desktop-debuginfo-2.6_k3.16.7_29-13.2
kernel-default-debuginfo-3.16.7-29.1
vhba-kmp-desktop-debuginfo-20140629_k3.16.7_29-2.13.2
xtables-addons-kmp-pae-debuginfo-2.6_k3.16.7_29-13.2
vhba-kmp-xen-20140629_k3.16.7_29-2.13.2
libipset3-6.23-13.2
pcfclock-debuginfo-0.44-260.13.2
xen-debugsource-4.4.2_06-27.2
kernel-default-base-debuginfo-3.16.7-29.1
cloop-kmp-desktop-2.639_k3.16.7_29-14.13.2
bbswitch-kmp-xen-debuginfo-0.8_k3.16.7_29-3.13.2
vhba-kmp-default-debuginfo-20140629_k3.16.7_29-2.13.2
crash-kmp-default-debuginfo-7.0.8_k3.16.7_29-13.2
hdjmod-kmp-desktop-debuginfo-1.28_k3.16.7_29-18.14.2
xtables-addons-2.6-13.2
vhba-kmp-desktop-20140629_k3.16.7_29-2.13.2
bbswitch-kmp-default-0.8_k3.16.7_29-3.13.2
hdjmod-kmp-pae-1.28_k3.16.7_29-18.14.2
bbswitch-kmp-xen-0.8_k3.16.7_29-3.13.2
cloop-debuginfo-2.639-14.13.2
kernel-obs-build-debugsource-3.16.7-29.2

cloop-kmp-desktop-debuginfo-2.639_k3.16.7_29-14.13.2
hdjmod-debugsource-1.28-18.14.2
vhba-kmp-pae-debuginfo-20140629_k3.16.7_29-2.13.2
xen-tools-domU-debuginfo-4.4.2_06-27.2
vhba-kmp-xen-debuginfo-20140629_k3.16.7_29-2.13.2
ipset-devel-6.23-13.2
crash-kmp-pae-7.0.8_k3.16.7_29-13.2
crash-kmp-xen-7.0.8_k3.16.7_29-13.2
crash-doc-7.0.8-13.2
xtables-addons-debugsource-2.6-13.2
vhba-kmp-debugsource-20140629-2.13.2
cloop-kmp-xen-2.639_k3.16.7_29-14.13.2
ipset-kmp-pae-6.23_k3.16.7_29-13.2
crash-gcore-7.0.8-13.2
ipset-kmp-pae-debuginfo-6.23_k3.16.7_29-13.2
bbswitch-kmp-pae-debuginfo-0.8_k3.16.7_29-3.13.2
pcfclock-kmp-desktop-0.44_k3.16.7_29-260.13.2
cloop-kmp-xen-debuginfo-2.639_k3.16.7_29-14.13.2
bbswitch-debugsource-0.8-3.13.2
xtables-addons-kmp-xen-2.6_k3.16.7_29-13.2

i686

kernel-debug-devel-3.16.7-29.1
kernel-debug-base-debuginfo-3.16.7-29.1
kernel-debug-debugsource-3.16.7-29.1
kernel-ec2-base-debuginfo-3.16.7-29.1
kernel-vanilla-devel-3.16.7-29.1
kernel-pae-base-debuginfo-3.16.7-29.1
kernel-desktop-debuginfo-3.16.7-29.1
kernel-desktop-base-3.16.7-29.1
kernel-pae-base-3.16.7-29.1
kernel-pae-debugsource-3.16.7-29.1
kernel-debug-3.16.7-29.1
kernel-ec2-debuginfo-3.16.7-29.1
kernel-pae-devel-3.16.7-29.1
kernel-xen-debuginfo-3.16.7-29.1
kernel-pae-3.16.7-29.1
kernel-debug-base-3.16.7-29.1
kernel-xen-debugsource-3.16.7-29.1
kernel-vanilla-debugsource-3.16.7-29.1
kernel-xen-3.16.7-29.1
kernel-pae-debuginfo-3.16.7-29.1
kernel-desktop-base-debuginfo-3.16.7-29.1
kernel-desktop-3.16.7-29.1
kernel-desktop-devel-3.16.7-29.1
kernel-ec2-debugsource-3.16.7-29.1
kernel-xen-base-debuginfo-3.16.7-29.1
kernel-xen-devel-3.16.7-29.1
kernel-debug-devel-debuginfo-3.16.7-29.1
kernel-debug-debuginfo-3.16.7-29.1
kernel-vanilla-debuginfo-3.16.7-29.1
kernel-vanilla-3.16.7-29.1
kernel-xen-base-3.16.7-29.1
kernel-desktop-debugsource-3.16.7-29.1

noarch

kernel-source-vanilla-3.16.7-29.1
kernel-devel-3.16.7-29.1
kernel-source-3.16.7-29.1
kernel-macros-3.16.7-29.1

kernel-docs-3.16.7-29.3

x86_64

kernel-default-debugsource-3.16.7-29.1

kernel-xen-debuginfo-3.16.7-29.1

crash-devel-7.0.8-13.2

ipset-6.23-13.2

ipset-kmp-xen-6.23_k3.16.7_29-13.2

xen-kmp-default-debuginfo-4.4.2_06_k3.16.7_29-27.2

cloop-kmp-default-2.639_k3.16.7_29-14.13.2

cloop-debugsource-2.639-14.13.2

crash-kmp-desktop-debuginfo-7.0.8_k3.16.7_29-13.2

cloop-2.639-14.13.2

ipset-debugsource-6.23-13.2

kernel-default-devel-3.16.7-29.1

xen-kmp-desktop-debuginfo-4.4.2_06_k3.16.7_29-27.2

pcfclock-0.44-260.13.2

kernel-debug-devel-debuginfo-3.16.7-29.1

kernel-desktop-devel-3.16.7-29.1

kernel-ec2-3.16.7-29.1

kernel-xen-base-debuginfo-3.16.7-29.1

bbswitch-kmp-desktop-0.8_k3.16.7_29-3.13.2

hdjmod-kmp-default-debuginfo-1.28_k3.16.7_29-18.14.2

kernel-obs-qa-xen-3.16.7-29.1

pcfclock-kmp-default-debuginfo-0.44_k3.16.7_29-260.13.2

kernel-debug-base-3.16.7-29.1

kernel-obs-build-3.16.7-29.2

kernel-ec2-base-debuginfo-3.16.7-29.1

xtables-addons-kmp-desktop-2.6_k3.16.7_29-13.2

bbswitch-kmp-desktop-debuginfo-0.8_k3.16.7_29-3.13.2

kernel-ec2-debugsource-3.16.7-29.1

crash-debuginfo-7.0.8-13.2

xtables-addons-kmp-xen-debuginfo-2.6_k3.16.7_29-13.2

kernel-obs-qa-3.16.7-29.1

crash-eppic-debuginfo-7.0.8-13.2

cloop-kmp-default-debuginfo-2.639_k3.16.7_29-14.13.2

bbswitch-kmp-default-debuginfo-0.8_k3.16.7_29-3.13.2

kernel-syms-3.16.7-29.1

pcfclock-kmp-desktop-debuginfo-0.44_k3.16.7_29-260.13.2

144021 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1835-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9749

Description

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

openSUSE-SU-2015:1835-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-10/msg00052.html>

SuSE Linux 13.1

x86_64

squid-debuginfo-3.3.13-2.23.1
squid-3.3.13-2.23.1
squid-debugsource-3.3.13-2.23.1

i586
squid-debuginfo-3.3.13-2.23.1
squid-3.3.13-2.23.1
squid-debugsource-3.3.13-2.23.1

SuSE Linux 13.2
x86_64
squid-debugsource-3.4.4-3.13.1
squid-debuginfo-3.4.4-3.13.1
squid-3.4.4-3.13.1

i586
squid-debugsource-3.4.4-3.13.1
squid-debuginfo-3.4.4-3.13.1
squid-3.4.4-3.13.1

144022 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1892-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5198, CVE-2015-5199, CVE-2015-5200

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1892-1

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/001664.html>

SuSE SLED 12
x86_64
libvdpau1-32bit-0.8-3.1
libvdpau1-0.8-3.1
libvdpau-debugsource-0.8-3.1
libvdpau1-debuginfo-32bit-0.8-3.1
libvdpau1-debuginfo-0.8-3.1

SuSE SLES 12
x86_64
libvdpau1-0.8-3.1
libvdpau-debugsource-0.8-3.1
libvdpau1-debuginfo-0.8-3.1

170583 - Amazon Linux AMI ALAS-2015-607 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7704, CVE-2015-7852, CVE-2015-7871

Description

The scan detected that the host is missing the following update:
ALAS-2015-607

Observation

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

<https://alas.aws.amazon.com/ALAS-2015-607.html>

Amazon Linux AMI

i686

ntpdate-4.2.6p5-34.27.amzn1

ntp-debuginfo-4.2.6p5-34.27.amzn1

ntp-4.2.6p5-34.27.amzn1

noarch

ntp-perl-4.2.6p5-34.27.amzn1

ntp-doc-4.2.6p5-34.27.amzn1

x86_64

ntpdate-4.2.6p5-34.27.amzn1

ntp-debuginfo-4.2.6p5-34.27.amzn1

ntp-4.2.6p5-34.27.amzn1

189881 - Fedora Linux 21 FEDORA-2015-3ca3f2138b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5198, CVE-2015-5199, CVE-2015-5200

Description

The scan detected that the host is missing the following update:
FEDORA-2015-3ca3f2138b

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/170637.html>

Fedora Core 21

libvdpa-1.1.1-2.fc21

189882 - Fedora Linux 22 FEDORA-2015-15767 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4499

Description

The scan detected that the host is missing the following update:
FEDORA-2015-15767

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169983.html>

Fedora Core 22

bugzilla-4.4.10-1.fc22

189884 - Fedora Linux 23 FEDORA-2015-f9864ecd8f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1867

Description

The scan detected that the host is missing the following update:
FEDORA-2015-f9864ecd8f

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169995.html>

Fedora Core 23

pacemaker-1.1.13-3.fc23

189887 - Fedora Linux 21 FEDORA-2015-15768 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4499

Description

The scan detected that the host is missing the following update:
FEDORA-2015-15768

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169946.html>

Fedora Core 21

bugzilla-4.4.10-1.fc21

189892 - Fedora Linux 21 FEDORA-2015-e5e36bbb87 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1867

Description

The scan detected that the host is missing the following update:
FEDORA-2015-e5e36bbb87

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/170610.html>

Fedora Core 21

pacemaker-1.1.13-3.fc21

189909 - Fedora Linux 23 FEDORA-2015-9f8f4b182a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1335

Description

The scan detected that the host is missing the following update:
FEDORA-2015-9f8f4b182a

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/170045.html>

Fedora Core 23

lxc-1.1.4-2.fc23

19170 - (HT205377) Apple Safari Multiple Vulnerabilities Prior To 9.0.1

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

Risk Level: Medium

CVE: CVE-2015-5928, CVE-2015-5929, CVE-2015-5930, CVE-2015-5931, CVE-2015-7002, CVE-2015-7011, CVE-2015-7012, CVE-2015-7013, CVE-2015-7014

Description

Multiple vulnerabilities are present in some versions of Apple Safari.

Observation

Apple Safari is a popular web browser.

Multiple vulnerabilities are present in some versions of Apple Safari. The flaws lie in WebKit component. Successful exploitation could allow an attacker to execute arbitrary code.

19187 - (JSA10707) Juniper Junos Corrupt Pam.conf File Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-7751

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is the operating system used in Juniper devices.

A vulnerability is present in some versions of Juniper Junos. The flaw is due to improper handling of corrupted pam.conf file. Successful exploitation could allow an attacker to bypass security measures and gain full access to the target device.

19192 - IBM AIX OpenSSH Multiple Vulnerabilities (openssh_advisory6)

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

Risk Level: Medium

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

Description

Two vulnerabilities are present in some versions of IBM AIX.

Observation

IBM AIX is a Unix-like operating system.

Two vulnerabilities are present in some versions of IBM AIX. The flaws lie in OpenSSH. Successful exploitation could allow a local attacker to conduct impersonation attacks or privilege escalation attacks.

91921 - Oracle Enterprise Linux ELSA-2015-1978 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

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/005488.html>

OEL7

x86_64

kernel-abi-whitelists-3.10.0-229.20.1.el7

kernel-debug-3.10.0-229.20.1.el7

perf-3.10.0-229.20.1.el7

kernel-tools-libs-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-doc-3.10.0-229.20.1.el7
kernel-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7

130300 - Debian Linux 7.0, 8.0 DSA-3388-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2014-9751, CVE-2015-3405, CVE-2015-5146, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7850, CVE-2015-7852, CVE-2015-7855, CVE-2015-7871

Description

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

DSA-3388-1

Observation

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

For more information see:

<http://www.debian.org/security/2015/dsa-3388>

Debian 8.0

all

ntp_1:4.2.6.p5+dfsg-7+deb8u1

Debian 7.0

all

ntp_1:4.2.6.p5+dfsg-2+deb7u6

130306 - Debian Linux 7.0, 8.0 DSA-3382-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8958, CVE-2014-9218, CVE-2015-2206, CVE-2015-3902, CVE-2015-3903, CVE-2015-6830, CVE-2015-7873

Description

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

DSA-3382-1

Observation

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

For more information see:

<http://www.debian.org/security/2015/dsa-3382>

Debian 8.0

all

phpmyadmin_4:4.2.12-2+deb8u1

Debian 7.0

all

phpmyadmin_4:3.4.11.1-2+deb7u2

140967 - Red Hat Enterprise Linux RHSA-2015-1978 Update Is Not Installed

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

Risk Level: Medium

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

Description

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

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-1978.html>

RHEL7D

x86_64
perf-3.10.0-229.20.1.el7
python-perf-3.10.0-229.20.1.el7
kernel-debug-3.10.0-229.20.1.el7
python-perf-debuginfo-3.10.0-229.20.1.el7
kernel-devel-3.10.0-229.20.1.el7
kernel-debuginfo-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.20.1.el7
kernel-debug-debuginfo-3.10.0-229.20.1.el7
kernel-tools-debuginfo-3.10.0-229.20.1.el7
kernel-tools-libs-devel-3.10.0-229.20.1.el7
perf-debuginfo-3.10.0-229.20.1.el7
kernel-debug-devel-3.10.0-229.20.1.el7
kernel-tools-3.10.0-229.20.1.el7
kernel-3.10.0-229.20.1.el7
kernel-tools-libs-3.10.0-229.20.1.el7

noarch

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

RHEL7S

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

x86_64

perf-3.10.0-229.20.1.el7
python-perf-3.10.0-229.20.1.el7
kernel-debug-3.10.0-229.20.1.el7
python-perf-debuginfo-3.10.0-229.20.1.el7
kernel-devel-3.10.0-229.20.1.el7
kernel-debuginfo-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.20.1.el7
kernel-debug-debuginfo-3.10.0-229.20.1.el7
kernel-tools-debuginfo-3.10.0-229.20.1.el7
kernel-tools-libs-devel-3.10.0-229.20.1.el7
perf-debuginfo-3.10.0-229.20.1.el7
kernel-debug-devel-3.10.0-229.20.1.el7
kernel-tools-3.10.0-229.20.1.el7

kernel-3.10.0-229.20.1.el7
kernel-tools-libs-3.10.0-229.20.1.el7

RHEL7WS

x86_64
perf-3.10.0-229.20.1.el7
python-perf-3.10.0-229.20.1.el7
kernel-debug-3.10.0-229.20.1.el7
python-perf-debuginfo-3.10.0-229.20.1.el7
kernel-devel-3.10.0-229.20.1.el7
kernel-debuginfo-3.10.0-229.20.1.el7
kernel-headers-3.10.0-229.20.1.el7
kernel-debuginfo-common-x86_64-3.10.0-229.20.1.el7
kernel-debug-debuginfo-3.10.0-229.20.1.el7
kernel-tools-debuginfo-3.10.0-229.20.1.el7
kernel-tools-libs-devel-3.10.0-229.20.1.el7
perf-debuginfo-3.10.0-229.20.1.el7
kernel-debug-devel-3.10.0-229.20.1.el7
kernel-tools-3.10.0-229.20.1.el7
kernel-3.10.0-229.20.1.el7
kernel-tools-libs-3.10.0-229.20.1.el7

noarch

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

144024 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1844-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8121, CVE-2015-1781

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1844-1

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-October/001651.html>

SuSE SLED 12

x86_64
glibc-locale-debuginfo-32bit-2.19-22.7.1
glibc-debuginfo-2.19-22.7.1
glibc-devel-debuginfo-2.19-22.7.1
glibc-locale-2.19-22.7.1
glibc-2.19-22.7.1
glibc-locale-debuginfo-2.19-22.7.1
glibc-devel-2.19-22.7.1
nscd-debuginfo-2.19-22.7.1
glibc-devel-32bit-2.19-22.7.1
glibc-debuginfo-32bit-2.19-22.7.1
nscd-2.19-22.7.1
glibc-locale-32bit-2.19-22.7.1
glibc-devel-debuginfo-32bit-2.19-22.7.1
glibc-32bit-2.19-22.7.1

glibc-debugsource-2.19-22.7.1

noarch

glibc-i18ndata-2.19-22.7.1

SuSE SLES 12

noarch

glibc-i18ndata-2.19-22.7.1

glibc-info-2.19-22.7.1

glibc-html-2.19-22.7.1

x86_64

glibc-locale-debuginfo-32bit-2.19-22.7.1

glibc-debuginfo-2.19-22.7.1

glibc-devel-debuginfo-2.19-22.7.1

glibc-locale-2.19-22.7.1

glibc-2.19-22.7.1

glibc-profile-32bit-2.19-22.7.1

glibc-locale-debuginfo-2.19-22.7.1

glibc-devel-2.19-22.7.1

nscd-debuginfo-2.19-22.7.1

glibc-devel-32bit-2.19-22.7.1

glibc-debuginfo-32bit-2.19-22.7.1

nscd-2.19-22.7.1

glibc-locale-32bit-2.19-22.7.1

glibc-devel-debuginfo-32bit-2.19-22.7.1

glibc-32bit-2.19-22.7.1

glibc-profile-2.19-22.7.1

glibc-debugsource-2.19-22.7.1

170584 - Amazon Linux AMI ALAS-2015-603 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2925, CVE-2015-7613

Description

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

ALAS-2015-603

Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2015-603.html>

Amazon Linux AMI

i686

kernel-tools-debuginfo-4.1.10-17.31.amzn1

kernel-tools-4.1.10-17.31.amzn1

perf-4.1.10-17.31.amzn1

perf-debuginfo-4.1.10-17.31.amzn1

kernel-devel-4.1.10-17.31.amzn1

kernel-debuginfo-4.1.10-17.31.amzn1

kernel-tools-devel-4.1.10-17.31.amzn1

kernel-debuginfo-common-i686-4.1.10-17.31.amzn1

kernel-headers-4.1.10-17.31.amzn1

kernel-4.1.10-17.31.amzn1

noarch
kernel-doc-4.1.10-17.31.amzn1

x86_64
kernel-tools-debuginfo-4.1.10-17.31.amzn1
kernel-headers-4.1.10-17.31.amzn1
kernel-tools-4.1.10-17.31.amzn1
kernel-debuginfo-4.1.10-17.31.amzn1
perf-debuginfo-4.1.10-17.31.amzn1
kernel-devel-4.1.10-17.31.amzn1
kernel-debuginfo-common-x86_64-4.1.10-17.31.amzn1
perf-4.1.10-17.31.amzn1
kernel-tools-devel-4.1.10-17.31.amzn1
kernel-4.1.10-17.31.amzn1

189879 - Fedora Linux 22 FEDORA-2015-7fcc957ba6 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2015-7fcc957ba6

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/170591.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170589.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170587.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170588.html>
<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170590.html>

Fedora Core 22

spice-0.12.6-1.fc22
spice-protocol-0.12.10-1.fc22
mingw-spice-protocol-0.12.10-1.fc22
spice-gtk-0.30-1.fc22
mingw-spice-gtk-0.30-1.fc22

189894 - Fedora Linux 23 FEDORA-2015-e22bb33731 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5291

Description

The scan detected that the host is missing the following update:
FEDORA-2015-e22bb33731

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/170317.html>

Fedora Core 23

mbdts-2.1.2-1.fc23

189911 - Fedora Linux 21 FEDORA-2015-d7e074ba30 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2015-d7e074ba30

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/170641.html>

Fedora Core 21

kernel-4.1.10-100.fc21

19183 - (JSA10701) Juniper Junos uBFD Packet Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-7748

Description

A vulnerability in some versions of Juniper Junos could lead to a denial of service.

Observation

A vulnerability in some versions of Juniper Junos could lead to a denial of service.

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

19186 - 3S CODESYS Gateway Null Pointer Exception Denial of Service

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

Risk Level: Medium

CVE: CVE-2015-6484

Description

A vulnerability in some versions of 3S CODESYS Gateway Server could lead to a denial of service.

Observation

A vulnerability in some versions of 3S CODESYS Gateway Server could lead to a denial of service.

The flaw lies in the handling of certain HTTP POST/GET requests. Successful exploitation by a remote attacker could result in a denial of service condition.

19189 - 3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-6482

Description

A denial of service condition is present in some versions of 3S CODESYS.

Observation

3S CODESYS is used for programming and creating controller applications that are used across the energy, critical manufacturing, and industrial automation industries.

A denial of service condition is present in some versions of 3S CODESYS. The flaw lies in the run-time toolkit. Successful exploitation could allow an attacker to cause a denial of service condition

19199 - Cisco ASA DHCPv6 Relay Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-0578

Description

A denial of service condition is present in some versions of Cisco ASA.

Observation

Cisco ASA Adaptive Security Appliances are the popular network security devices developed by Cisco.

A denial of service condition is present in some versions of Cisco ASA. The flaw lies in the DHCPv6 relay. Successful exploitation could allow an attacker to cause a denial of service condition.

85996 - CentOS 7 CESA-2015-1943 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1779

Description

The scan detected that the host is missing the following update:
CESA-2015-1943

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-October/021449.html>

CentOS 7
x86_64
libcacard-tools-1.5.3-86.el7_1.8
qemu-kvm-1.5.3-86.el7_1.8
qemu-kvm-common-1.5.3-86.el7_1.8
qemu-img-1.5.3-86.el7_1.8
libcacard-devel-1.5.3-86.el7_1.8
qemu-kvm-tools-1.5.3-86.el7_1.8
libcacard-1.5.3-86.el7_1.8

i686
libcacard-1.5.3-86.el7_1.8
libcacard-devel-1.5.3-86.el7_1.8

85997 - CentOS 7 CESA-2015-1979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3240

Description

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

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/021462.html>

CentOS 7
x86_64
libreswan-3.15-5.el7_1

88715 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2015-302-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5196, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855, CVE-2015-7871

Description

The scan detected that the host is missing the following update:
SSA:2015-302-03

Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.581166>

Slackware 14.0
x86_64
ntp-4.2.8p4-x86_64-1

Slackware 13.0
x86_64
ntp-4.2.8p4-x86_64-1

Slackware 13.1
x86_64
ntp-4.2.8p4-x86_64-1

Slackware 14.1
x86_64
ntp-4.2.8p4-x86_64-1

Slackware 13.37
x86_64
ntp-4.2.8p4-x86_64-1

91922 - Oracle Enterprise Linux ELSA-2015-1979 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3240

Description

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

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/005489.html>

OEL7
x86_64
libreswan-3.15-5.0.1.el7_1

130302 - Debian Linux 7.0, 8.0 DSA-3384-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4813, CVE-2015-4896

Description

The scan detected that the host is missing the following update:
DSA-3384-1

Observation

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

<http://www.debian.org/security/2015/dsa-3384>

Debian 8.0
all
virtualbox_4.3.32-dfsg-1+deb8u2

Debian 7.0
all
virtualbox_4.1.42-dfsg-1+deb7u1

144023 - SuSE SLES 12 SUSE-SU-2015:1851-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8111, CVE-2015-3183, CVE-2015-3185, CVE-2015-4000

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1851-1

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-October/001653.html>

SuSE SLES 12
noarch
apache2-doc-2.4.10-14.10.1

x86_64
apache2-prefork-2.4.10-14.10.1
apache2-debugsource-2.4.10-14.10.1
apache2-utils-debuginfo-2.4.10-14.10.1
apache2-utils-2.4.10-14.10.1
apache2-mod_jk-debuginfo-1.2.40-2.6.1
apache2-prefork-debuginfo-2.4.10-14.10.1
apache2-worker-2.4.10-14.10.1
apache2-mod_jk-debugsource-1.2.40-2.6.1
apache2-mod_jk-1.2.40-2.6.1
apache2-2.4.10-14.10.1
apache2-worker-debuginfo-2.4.10-14.10.1
apache2-mod_security2-debuginfo-2.8.0-3.4.1
apache2-mod_auth_kerb-debugsource-5.4-2.4.1
apache2-debuginfo-2.4.10-14.10.1
apache2-mod_auth_kerb-5.4-2.4.1
apache2-mod_security2-debugsource-2.8.0-3.4.1
apache2-mod_security2-2.8.0-3.4.1
apache2-example-pages-2.4.10-14.10.1
apache2-mod_auth_kerb-debuginfo-5.4-2.4.1

144025 - SuSE Linux 13.2 openSUSE-SU-2015:1855-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4813, CVE-2015-4896

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1855-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00000.html>

SuSE Linux 13.2

i586

virtualbox-guest-kmp-pae-4.3.32_k3.16.7_29-32.2
virtualbox-devel-4.3.32-32.2
virtualbox-4.3.32-32.2
virtualbox-host-kmp-default-4.3.32_k3.16.7_29-32.2
virtualbox-host-kmp-desktop-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-qt-4.3.32-32.2
virtualbox-guest-kmp-desktop-4.3.32_k3.16.7_29-32.2
virtualbox-guest-tools-4.3.32-32.2
virtualbox-host-kmp-pae-debuginfo-4.3.32_k3.16.7_29-32.2
python-virtualbox-4.3.32-32.2
virtualbox-guest-kmp-desktop-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-debugsource-4.3.32-32.2
python-virtualbox-debuginfo-4.3.32-32.2
virtualbox-host-kmp-default-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-websrv-debuginfo-4.3.32-32.2
virtualbox-websrv-4.3.32-32.2
virtualbox-host-kmp-desktop-4.3.32_k3.16.7_29-32.2
virtualbox-guest-x11-4.3.32-32.2
virtualbox-guest-kmp-default-4.3.32_k3.16.7_29-32.2
virtualbox-debuginfo-4.3.32-32.2
virtualbox-guest-kmp-pae-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-guest-kmp-default-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-guest-x11-debuginfo-4.3.32-32.2
virtualbox-guest-tools-debuginfo-4.3.32-32.2
virtualbox-qt-debuginfo-4.3.32-32.2
virtualbox-host-kmp-pae-4.3.32_k3.16.7_29-32.2

noarch

virtualbox-guest-desktop-icons-4.3.32-32.2
virtualbox-host-source-4.3.32-32.2

x86_64

virtualbox-devel-4.3.32-32.2
virtualbox-4.3.32-32.2
virtualbox-host-kmp-default-4.3.32_k3.16.7_29-32.2
virtualbox-host-kmp-desktop-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-qt-4.3.32-32.2
virtualbox-guest-kmp-desktop-4.3.32_k3.16.7_29-32.2
virtualbox-guest-tools-4.3.32-32.2
python-virtualbox-4.3.32-32.2
virtualbox-guest-kmp-desktop-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-debugsource-4.3.32-32.2
python-virtualbox-debuginfo-4.3.32-32.2
virtualbox-host-kmp-default-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-websrv-debuginfo-4.3.32-32.2
virtualbox-websrv-4.3.32-32.2
virtualbox-host-kmp-desktop-4.3.32_k3.16.7_29-32.2
virtualbox-guest-x11-4.3.32-32.2
virtualbox-guest-kmp-default-4.3.32_k3.16.7_29-32.2
virtualbox-debuginfo-4.3.32-32.2
virtualbox-guest-kmp-default-debuginfo-4.3.32_k3.16.7_29-32.2
virtualbox-guest-x11-debuginfo-4.3.32-32.2
virtualbox-guest-tools-debuginfo-4.3.32-32.2

189915 - Fedora Linux 22 FEDORA-2015-17908c56c1 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-2015-17908c56c1

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169986.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169987.html>

Fedora Core 22

phpMyAdmin-4.5.1-1.fc22

php-udan11-sql-parser-3.0.4-1.fc22

18555 - WordPress S3 Video Plugin Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-7279

Description

A Cross-site scripting vulnerability is present in some versions of S3 video Plugin for WordPress.

Observation

WordPress is a popular blog web application.

A Cross-site scripting vulnerability is present in some versions of S3 video Plugin for WordPress. The flaw lies in the views/video-management/preview_video.php file. Successful exploitation could allow an attacker to execute remote code.

144019 - SuSE SLES 12, SLED 12 SUSE-SU-2015:1838-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3218, CVE-2015-3255, CVE-2015-3256, CVE-2015-4625

Description

The scan detected that the host is missing the following update:
SUSE-SU-2015:1838-1

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-October/001649.html>

SuSE SLED 12

x86_64
libpolkit0-0.113-4.1
typelib-1_0-Polkit-1_0-0.113-4.1
polkit-0.113-4.1
polkit-debugsource-0.113-4.1
libpolkit0-debuginfo-0.113-4.1
libpolkit0-debuginfo-32bit-0.113-4.1
libpolkit0-32bit-0.113-4.1
polkit-debuginfo-0.113-4.1

SuSE SLES 12

x86_64
libpolkit0-0.113-4.1
libpolkit0-debuginfo-0.113-4.1
typelib-1_0-Polkit-1_0-0.113-4.1
polkit-0.113-4.1
polkit-debugsource-0.113-4.1
polkit-debuginfo-0.113-4.1

144020 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:1836-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6241, CVE-2015-6242, CVE-2015-6243, CVE-2015-6244, CVE-2015-6245, CVE-2015-6246, CVE-2015-6247, CVE-2015-6248, CVE-2015-6249, CVE-2015-7830

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2015:1836-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-10/msg00053.html>

SuSE Linux 13.1

x86_64
wireshark-1.12.8-43.1
wireshark-ui-gtk-1.12.8-43.1
wireshark-ui-qt-1.12.8-43.1
wireshark-ui-qt-debuginfo-1.12.8-43.1
wireshark-debuginfo-1.12.8-43.1
wireshark-ui-gtk-debuginfo-1.12.8-43.1
wireshark-debugsource-1.12.8-43.1
wireshark-devel-1.12.8-43.1

i586

wireshark-1.12.8-43.1
wireshark-ui-gtk-1.12.8-43.1
wireshark-ui-qt-1.12.8-43.1
wireshark-ui-qt-debuginfo-1.12.8-43.1
wireshark-debuginfo-1.12.8-43.1
wireshark-ui-gtk-debuginfo-1.12.8-43.1
wireshark-debugsource-1.12.8-43.1

wireshark-devel-1.12.8-43.1

SuSE Linux 13.2

x86_64

wireshark-debuginfo-1.12.8-25.1

wireshark-ui-qt-debuginfo-1.12.8-25.1

wireshark-ui-gtk-1.12.8-25.1

wireshark-debugsource-1.12.8-25.1

wireshark-ui-gtk-debuginfo-1.12.8-25.1

wireshark-1.12.8-25.1

wireshark-ui-qt-1.12.8-25.1

wireshark-devel-1.12.8-25.1

i586

wireshark-debuginfo-1.12.8-25.1

wireshark-ui-qt-debuginfo-1.12.8-25.1

wireshark-ui-gtk-1.12.8-25.1

wireshark-debugsource-1.12.8-25.1

wireshark-ui-gtk-debuginfo-1.12.8-25.1

wireshark-1.12.8-25.1

wireshark-ui-qt-1.12.8-25.1

wireshark-devel-1.12.8-25.1

130305 - Debian Linux 7.0, 8.0 DSA-3387-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7762, CVE-2015-7763

Description

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

DSA-3387-1

Observation

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

For more information see:

<http://www.debian.org/security/2015/dsa-3387>

Debian 8.0

all

libafsrpc1_1.6.9-2+deb8u4

libpam-openafs-kaserver_1.6.9-2+deb8u4

openafs-kpasswd_1.6.9-2+deb8u4

libafsauthent1_1.6.9-2+deb8u4

libkopenafs1_1.6.9-2+deb8u4

openafs-dbg_1.6.9-2+deb8u4

openafs-modules-source_1.6.9-2+deb8u4

openafs-client_1.6.9-2+deb8u4

openafs-doc_1.6.9-2+deb8u4

openafs-modules-dkms_1.6.9-2+deb8u4

openafs-fileserver_1.6.9-2+deb8u4

openafs-dbserver_1.6.9-2+deb8u4

libopenafs-dev_1.6.9-2+deb8u4

openafs-krb5_1.6.9-2+deb8u4

openafs-fuse_1.6.9-2+deb8u4

Debian 7.0

all
openafs-client_1.6.1-3+deb7u5
libkopenafs1_1.6.1-3+deb7u5
openafs-modules-dkms_1.6.1-3+deb7u5
openafs-fileserver_1.6.1-3+deb7u5
libopenafs-dev_1.6.1-3+deb7u5
openafs-krb5_1.6.1-3+deb7u5
openafs-fuse_1.6.1-3+deb7u5
openafs-modules-source_1.6.1-3+deb7u5
libafsrpc1_1.6.1-3+deb7u5
openafs-kpasswd_1.6.1-3+deb7u5
openafs-dbserver_1.6.1-3+deb7u5
openafs-doc_1.6.1-3+deb7u5
openafs-dbg_1.6.1-3+deb7u5
libafsauthent1_1.6.1-3+deb7u5
libpam-openafs-kaserver_1.6.1-3+deb7u5

130307 - Debian Linux 7.0, 8.0 DSA-3383-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-2213, CVE-2015-5622, CVE-2015-5714, CVE-2015-5715, CVE-2015-5731, CVE-2015-5732, CVE-2015-5734, CVE-2015-7989

Description

The scan detected that the host is missing the following update:
DSA-3383-1

Observation

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

<http://www.debian.org/security/2015/dsa-3383>

Debian 8.0
all
wordpress_4.1+dfsg-1+deb8u5

Debian 7.0
all
wordpress_3.6.1+dfsg-1~deb7u8

130308 - Debian Linux 7.0, 8.0 DSA-3386-1 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
DSA-3386-1

Observation

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

<http://www.debian.org/security/2015/dsa-3386>

Debian 8.0
all
unzip_6.0-16+deb8u1

Debian 7.0
all
unzip_6.0-8+deb7u4

140966 - Red Hat Enterprise Linux RHSA-2015-1955 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2015-1955

Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-1955.html>

RHEL6_5S
i386
redhat-release-server-6Server-6.5.0.3.el6_5.1

x86_64
redhat-release-server-6Server-6.5.0.3.el6_5.1

181659 - FreeBSD openafs Information Disclosure (017a493f-7db6-11e5-a762-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-7762, CVE-2015-7763

Description

The scan detected that the host is missing the following update:
openafs -- information disclosure (017a493f-7db6-11e5-a762-14dae9d210b8)

Observation

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

<http://www.vuxml.org/freebsd/017a493f-7db6-11e5-a762-14dae9d210b8.html>

Affected packages:
openafs < 1.6.15

181660 - FreeBSD codeigniter Multiple Vulnerabilities (698403a7-803d-11e5-ab94-002590263bf5)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

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

codeigniter -- multiple vulnerabilities (698403a7-803d-11e5-ab94-002590263bf5)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/698403a7-803d-11e5-ab94-002590263bf5.html>

Affected packages:

codeigniter < 2.2.6

185029 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2788-1 Update Is Not Installed

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

Risk Level: Low

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

Description

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

USN-2788-1

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-October/003168.html>

Ubuntu 12.04

unzip_6.0-4ubuntu2.4

Ubuntu 15.04

unzip_6.0-13ubuntu3.1

Ubuntu 15.10

unzip_6.0-17ubuntu1.1

Ubuntu 14.04

unzip_6.0-9ubuntu1.4

185031 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2786-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7803, CVE-2015-7804

Description

The scan detected that the host is missing the following update:
USN-2786-1

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-October/003166.html>

Ubuntu 12.04

php5-fpm_5.3.10-1ubuntu3.21
php5-cli_5.3.10-1ubuntu3.21
libapache2-mod-php5_5.3.10-1ubuntu3.21
php5-cgi_5.3.10-1ubuntu3.21

Ubuntu 15.04

libapache2-mod-php5_5.6.4+dfsg-4ubuntu6.4
php5-cgi_5.6.4+dfsg-4ubuntu6.4
php5-cli_5.6.4+dfsg-4ubuntu6.4
php5-fpm_5.6.4+dfsg-4ubuntu6.4

Ubuntu 15.10

php5-cgi_5.6.11+dfsg-1ubuntu3.1
php5-cli_5.6.11+dfsg-1ubuntu3.1
libapache2-mod-php5_5.6.11+dfsg-1ubuntu3.1
php5-fpm_5.6.11+dfsg-1ubuntu3.1

Ubuntu 14.04

php5-cli_5.5.9+dfsg-1ubuntu4.14
php5-cgi_5.5.9+dfsg-1ubuntu4.14
libapache2-mod-php5_5.5.9+dfsg-1ubuntu4.14
php5-fpm_5.5.9+dfsg-1ubuntu4.14

185032 - Ubuntu Linux 12.04 USN-2789-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8025

Description

The scan detected that the host is missing the following update:
USN-2789-1

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/003169.html>

Ubuntu 12.04

xscreensaver_5.15-2ubuntu1.1

185033 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2787-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7747

Description

The scan detected that the host is missing the following update:
USN-2787-1

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-October/003167.html>

Ubuntu 12.04

libaudiofile1_0.3.3-2ubuntu0.1

Ubuntu 15.04

libaudiofile1_0.3.6-2ubuntu0.15.04.1

Ubuntu 15.10

libaudiofile1_0.3.6-2ubuntu0.15.10.1

Ubuntu 14.04

libaudiofile1_0.3.6-2ubuntu0.14.04.1

189874 - Fedora Linux 23 FEDORA-2015-c7b2a6564b 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-c7b2a6564b

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/170035.html>

Fedora Core 23

seqan-1.4.2-21.fc23

189875 - Fedora Linux 23 FEDORA-2015-1f4cde17c4 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-2015-1f4cde17c4

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/170364.html>

Fedora Core 23

drupal7-jquery_update-2.6-1.fc23

189876 - Fedora Linux 23 FEDORA-2015-19b2b73dc5 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-2015-19b2b73dc5

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/170682.html>

Fedora Core 23

xscreensaver-5.34-1.fc23

189877 - Fedora Linux 23 FEDORA-2015-1661d2d6bf 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-2015-1661d2d6bf

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/170144.html>

Fedora Core 23

189878 - Fedora Linux 22 FEDORA-2015-693035254a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5211

Description

The scan detected that the host is missing the following update:
FEDORA-2015-693035254a

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/170543.html>

Fedora Core 22

springframework-3.2.15-1.fc22

189880 - Fedora Linux 22 FEDORA-2015-b81f7e1e86 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5302

Description

The scan detected that the host is missing the following update:
FEDORA-2015-b81f7e1e86

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169962.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169961.html>

Fedora Core 22

libreport-2.6.3-1.fc22

abrt-2.6.1-6.fc22

189883 - Fedora Linux 23 FEDORA-2015-3a59e6cf5c 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-2015-3a59e6cf5c

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/170032.html>

Fedora Core 23

libsbw-2.11.1-9.20150414svn579.fc23

189885 - Fedora Linux 21 FEDORA-2015-111f449417 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-2015-111f449417

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/170643.html>

Fedora Core 21

community-mysql-5.6.27-1.fc21

189886 - Fedora Linux 23 FEDORA-2015-44deeee4d7a 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-2015-44deeee4d7a

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/170417.html>

Fedora Core 23

lxdm-0.5.1-7.D20151007gite8f38708.fc23

189888 - Fedora Linux 23 FEDORA-2015-ccf2b449a9 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-ccf2b449a9

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/170686.html>

Fedora Core 23

drupal7-7.41-1.fc23

189889 - Fedora Linux 22 FEDORA-2015-27cfe187b5 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-2015-27cfe187b5

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169948.html>

Fedora Core 22

java-1.8.0-openjdk-1.8.0.65-3.b17.fc22

189890 - Fedora Linux 21 FEDORA-2015-9295d75400 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5211

Description

The scan detected that the host is missing the following update:
FEDORA-2015-9295d75400

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/170611.html>

Fedora Core 21

springframework-3.2.15-1.fc21

189891 - Fedora Linux 23 FEDORA-2015-be1b87a3b7 Update Is Not Installed

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

Risk Level: Low

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

Description

The scan detected that the host is missing the following update:
FEDORA-2015-be1b87a3b7

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/170683.html>

Fedora Core 23

krb5-1.13.2-12.fc23

189893 - Fedora Linux 23 FEDORA-2015-05b74288af 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-2015-05b74288af

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/170681.html>

Fedora Core 23

git-2.5.0-2.fc23

189895 - Fedora Linux 22 FEDORA-2015-b689ef0dbf 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-b689ef0dbf

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/170598.html>

Fedora Core 22

community-mysql-5.6.27-1.fc22

189896 - Fedora Linux 23 FEDORA-2015-02382803f3 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-2015-02382803f3

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/170463.html>

Fedora Core 23

community-mysql-5.6.27-1.fc23

189897 - Fedora Linux 23 FEDORA-2015-8d643c4d18 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-2015-8d643c4d18

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/170437.html>

Fedora Core 23

squid-3.5.9-7.fc23

189898 - Fedora Linux 23 FEDORA-2015-065d9953e8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5211

Description

The scan detected that the host is missing the following update:
FEDORA-2015-065d9953e8

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/170077.html>

Fedora Core 23

springframework-3.2.15-1.fc23

189899 - Fedora Linux 21 FEDORA-2015-54365c8fc7 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-2015-54365c8fc7

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/170709.html>

Fedora Core 21

drupal7-7.41-1.fc21

189900 - Fedora Linux 23 FEDORA-2015-ed1c673f09 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7687

Description

The scan detected that the host is missing the following update:
FEDORA-2015-ed1c673f09

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/170448.html>

Fedora Core 23

opensmtpd-5.7.3p1-1.fc23

189901 - Fedora Linux 22 FEDORA-2015-13616 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3277

Description

The scan detected that the host is missing the following update:
FEDORA-2015-13616

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/170607.html>

Fedora Core 22

mod_nss-1.0.11-4.fc22

189902 - Fedora Linux 23 FEDORA-2015-de8ba28354 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-6816

Description

The scan detected that the host is missing the following update:
FEDORA-2015-de8ba28354

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/170362.html>

Fedora Core 23

ganglia-3.7.2-6.fc23

189903 - Fedora Linux 23 FEDORA-2015-d95ea78616 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-d95ea78616

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/170311.html>

Fedora Core 23

seamonkey-2.38-1.fc23

189904 - Fedora Linux 23 FEDORA-2015-b99b854d39 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-b99b854d39

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/170178.html>

Fedora Core 23

drupal7-active_tags-2.0-0.9.alpha1.fc23

189905 - Fedora Linux 23 FEDORA-2015-46c331cb4e 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-2015-46c331cb4e

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/170692.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170690.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170689.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/170691.html>

Fedora Core 23

php-horde-imp-6.2.11-1.fc23

php-horde-ingo-3.2.7-1.fc23

php-horde-passwd-5.0.4-1.fc23

php-horde-horde-5.2.8-1.fc23

189906 - Fedora Linux 23 FEDORA-2015-13919 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

Description

The scan detected that the host is missing the following update:
FEDORA-2015-13919

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/170523.html>

Fedora Core 23

ipsilon-1.0.0-5.fc23

189907 - Fedora Linux 23 FEDORA-2015-b15b90eeaa Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0856

Description

The scan detected that the host is missing the following update:
FEDORA-2015-b15b90eeaa

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169999.html>

Fedora Core 23

sddm-0.12.0-5.fc23

189908 - Fedora Linux 23 FEDORA-2015-cc585b503f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5302

Description

The scan detected that the host is missing the following update:
FEDORA-2015-cc585b503f

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169996.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169997.html>

Fedora Core 23

libreport-2.6.3-1.fc23

abrt-2.7.0-2.fc23

189910 - Fedora Linux 23 FEDORA-2015-605cd28f33 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7747

Description

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

FEDORA-2015-605cd28f33

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/170387.html>

Fedora Core 23

audiofile-0.3.6-9.fc23

189912 - Fedora Linux 23 FEDORA-2015-7a8067b88d 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-2015-7a8067b88d

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/170046.html>

Fedora Core 23

java-1.8.0-openjdk-1.8.0.65-3.b17.fc23

189913 - Fedora Linux 23 FEDORA-2015-16197 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-2015-16197

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/170497.html>

Fedora Core 23

python-tornado-4.2.1-1.fc23

189914 - Fedora Linux 23 FEDORA-2015-f5f5ec7b6b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7704, CVE-2015-7852, CVE-2015-7871

Description

The scan detected that the host is missing the following update:
FEDORA-2015-f5f5ec7b6b

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/170684.html>

Fedora Core 23

ntp-4.2.6p5-34.fc23

189916 - Fedora Linux 21 FEDORA-2015-ce54f85a3e 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-ce54f85a3e

Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-October/169926.html>

Fedora Core 21

java-1.8.0-openjdk-1.8.0.65-3.b17.fc21

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.

18192 - Adobe ColdFusion Authentication Controls Remote Code Execution II

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

Risk Level: High

CVE: CVE-2013-0632

Update Details

FASLScript is updated

18740 - (SOL16912) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4620

Update Details

FASLScript is updated

18743 - (SOL16909) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5477

Update Details

FASLScript is updated

18876 - Microsoft HTML Help Compiler Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

18903 - VideoLAN VLC Media Player 3GP File Arbitrary Pointer Dereference Vulnerability

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

Risk Level: High

CVE: CVE-2015-5949

Update Details

Recommendation is updated

19014 - (SOL17181) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High
CVE: CVE-2015-5722

[Update Details](#)

Recommendation is updated

130226 - Debian Linux 8.0 DSA-3307-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5470

[Update Details](#)

Risk is updated

130227 - Debian Linux 8.0 DSA-3306-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5470

[Update Details](#)

Risk is updated

170547 - Amazon Linux AMI ALAS-2015-567 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3230

[Update Details](#)

Risk is updated

181654 - FreeBSD Joomla! Core - SQL Injection/ACL Violation Vulnerabilities (0ebc6e78-7ac6-11e5-b35a-002590263bf5)

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

Risk Level: High

CVE: CVE-2015-7297, CVE-2015-7857, CVE-2015-7858, CVE-2015-7859

[Update Details](#)

Risk is updated

189818 - Fedora Linux 21 FEDORA-2015-15128 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3230

[Update Details](#)

Risk is updated

130298 - Debian Linux 7.0, 8.0 DSA-3379-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6031

Update Details

Risk is updated

181633 - FreeBSD miniupnpc Buffer Overflow (06fef2f-728f-11e5-a371-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2015-6031

Update Details

Risk is updated

181635 - FreeBSD mbedTLS/PolarSSL DoS And Possible Remote Code Execution (07a1a76c-734b-11e5-ae81-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2015-5291

Update Details

Risk is updated

185023 - Ubuntu Linux 12.04, 14.04, 15.04 USN-2780-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6031

Update Details

Risk is updated

185027 - Ubuntu Linux 15.10 USN-2780-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-6031

Update Details

Risk is updated

189833 - Fedora Linux 22 FEDORA-2015-7b47df69d3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

[Update Details](#)

Risk is updated

189843 - Fedora Linux 23 FEDORA-2015-202c127199 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

[Update Details](#)

Risk is updated

189852 - Fedora Linux 21 FEDORA-2015-30a417bea9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5291

[Update Details](#)

Risk is updated

189858 - Fedora Linux 21 FEDORA-2015-cdea5324a8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5292

[Update Details](#)

Risk is updated

189868 - Fedora Linux 22 FEDORA-2015-7f939b3af5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5291

[Update Details](#)

Risk is updated

181650 - FreeBSD Joomla! Core - ACL Violation Vulnerabilities (03e54e42-7ac6-11e5-b35a-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-7899

[Update Details](#)

Risk is updated

33178 - Oracle Solaris 137204-36 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

33180 - Oracle Solaris 137205-36 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

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

130292 - Debian Linux 8.0 DSA-3375-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5714, CVE-2015-5715, CVE-2015-7989

Update Details

CVE is updated

181598 - FreeBSD wordpress Multiple Vulnerabilities (f4ce64c2-5bd4-11e5-9040-3c970e169bc2)

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

Risk Level: Low

CVE: CVE-2015-5714, CVE-2015-5715, CVE-2015-7989

Update Details

CVE is updated

70055 - wordpress.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category

and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2015 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates