

## 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

#### 17529 - (VMSA-2014-0012) VMware vCenter Update Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2014-4209, CVE-2014-4216, CVE-2014-4218, CVE-2014-4219, CVE-2014-4227, CVE-2014-4244, CVE-2014-4252, CVE-2014-4262, CVE-2014-4263, CVE-2014-4265, CVE-2014-4268

#### Description

Multiple vulnerabilities are present in some versions of VMware vSphere Update Manager.

#### Observation

VMware vSphere Update Manager automates the patch management process of VMware vSphere hosts.

Multiple vulnerabilities are present in some versions of VMware vSphere Update Manager. The flaws lie in the embedded Oracle Java. Successful exploitation could allow an attacker to execute remote code.

#### 85845 - CentOS 7 CESA-2014-1976 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

#### Description

The scan detected that the host is missing the following update:  
CESA-2014-1976

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020821.html>

CentOS 7  
x86\_64  
rpm-build-4.11.1-18.el7\_0  
rpm-devel-4.11.1-18.el7\_0  
rpm-build-libs-4.11.1-18.el7\_0  
rpm-4.11.1-18.el7\_0  
rpm-sign-4.11.1-18.el7\_0  
rpm-libs-4.11.1-18.el7\_0  
rpm-python-4.11.1-18.el7\_0

rpm-libs-4.11.1-18.el7\_0  
rpm-devel-4.11.1-18.el7\_0  
rpm-build-libs-4.11.1-18.el7\_0

noarch  
rpm-cron-4.11.1-18.el7\_0  
rpm-apidocs-4.11.1-18.el7\_0

## 91686 - Oracle Enterprise Linux ELSA-2014-1976 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1976

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004708.html>

OEL7  
x86\_64  
rpm-build-libs-4.11.1-18.el7\_0  
rpm-sign-4.11.1-18.el7\_0  
rpm-4.11.1-18.el7\_0  
rpm-devel-4.11.1-18.el7\_0  
rpm-cron-4.11.1-18.el7\_0  
rpm-build-4.11.1-18.el7\_0  
rpm-python-4.11.1-18.el7\_0  
rpm-apidocs-4.11.1-18.el7\_0  
rpm-libs-4.11.1-18.el7\_0

## 93438 - Mandriva Linux MBS1 MDVSA-2014-251 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-251

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A251/>

Mandriva Linux mbs1  
x86\_64  
python-rpm-4.9.1.3-4.2  
rpm-sign-4.9.1.3-4.2

lib64rpmsign2-4.9.1.3-4.2  
rpm-build-4.9.1.3-4.2  
lib64rpmbuild2-4.9.1.3-4.2  
lib64rpm2-4.9.1.3-4.2  
lib64rpm-devel-4.9.1.3-4.2  
rpm-4.9.1.3-4.2

## 140644 - Red Hat Enterprise Linux RHSA-2014-1981 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

### Description

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

RHSA-2014-1981

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-1981.html>

#### RHEL5D

x86\_64

flash-plugin-11.2.202.425-1.el5

i386

flash-plugin-11.2.202.425-1.el5

#### RHEL5S

x86\_64

flash-plugin-11.2.202.425-1.el5

i386

flash-plugin-11.2.202.425-1.el5

#### RHEL6D

x86\_64

flash-plugin-11.2.202.425-1.el6

i386

flash-plugin-11.2.202.425-1.el6

#### RHEL6S

x86\_64

flash-plugin-11.2.202.425-1.el6

i386

flash-plugin-11.2.202.425-1.el6

#### RHEL6WS

x86\_64

flash-plugin-11.2.202.425-1.el6

i386

flash-plugin-11.2.202.425-1.el6

## 142563 - SuSE Linux 13.1 openSUSE-SU-2014:1638-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6629, CVE-2013-6954, CVE-2014-0429, CVE-2014-0446, CVE-2014-0451, CVE-2014-0452, CVE-2014-0453, CVE-2014-0454, CVE-2014-0455, CVE-2014-0456, CVE-2014-0457, CVE-2014-0458, CVE-2014-0459, CVE-2014-0460, CVE-2014-0461, CVE-2014-1876, CVE-2014-2397, CVE-2014-2398, CVE-2014-2402, CVE-2014-2403, CVE-2014-2412, CVE-2014-2413, CVE-2014-2414, CVE-2014-2421, CVE-2014-2423, CVE-2014-2427, CVE-2014-2483, CVE-2014-2490, CVE-2014-4209, CVE-2014-4216, CVE-2014-4218, CVE-2014-4219, CVE-2014-4221, CVE-2014-4223, CVE-2014-4244, CVE-2014-4252, CVE-2014-4262, CVE-2014-4263, CVE-2014-4264, CVE-2014-4266, CVE-2014-4268

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1638-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00056.html>

SuSE Linux 13.1

i586

java-1\_7\_0-openjdk-javadoc-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-src-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-devel-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-accessibility-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-debugsource-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-demo-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-headless-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-debuginfo-1.7.0.55-24.17.1

java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.55-24.17.1

## 142565 - SuSE SLED 11 SP3 flash-player-10090 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

### Description

The scan detected that the host is missing the following update:  
flash-player-10090

### Observation

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

<https://download.suse.com/Download?buildid=V5yWOD19QDc~>

<https://download.suse.com/Download?buildid=NVNjbksx3gQ~>

SuSE SLED 11 SP3

x86\_64

flash-player-kde4-11.2.202.425-0.3.1

flash-player-gnome-11.2.202.425-0.3.1  
flash-player-11.2.202.425-0.3.1

i586

flash-player-kde4-11.2.202.425-0.3.1  
flash-player-gnome-11.2.202.425-0.3.1  
flash-player-11.2.202.425-0.3.1

## 142569 - SuSE Linux 12.3 openSUSE-SU-2014:1645-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6629, CVE-2013-6954, CVE-2014-0429, CVE-2014-0446, CVE-2014-0451, CVE-2014-0452, CVE-2014-0453, CVE-2014-0454, CVE-2014-0455, CVE-2014-0456, CVE-2014-0457, CVE-2014-0458, CVE-2014-0459, CVE-2014-0460, CVE-2014-0461, CVE-2014-1876, CVE-2014-2397, CVE-2014-2398, CVE-2014-2402, CVE-2014-2403, CVE-2014-2412, CVE-2014-2413, CVE-2014-2414, CVE-2014-2421, CVE-2014-2423, CVE-2014-2427, CVE-2014-2483, CVE-2014-2490, CVE-2014-4209, CVE-2014-4216, CVE-2014-4218, CVE-2014-4219, CVE-2014-4221, CVE-2014-4223, CVE-2014-4244, CVE-2014-4252, CVE-2014-4262, CVE-2014-4263, CVE-2014-4264, CVE-2014-4266, CVE-2014-4268

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1645-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00063.html>

SuSE Linux 12.3

i586

java-1\_7\_0-openjdk-headless-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-accessibility-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-src-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-demo-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-javadoc-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-debugsource-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-devel-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.55-8.36.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.55-8.36.1

## 142570 - SuSE Linux 13.1, 13.2 openSUSE-SU-2014:1626-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0574, CVE-2014-7899, CVE-2014-7900, CVE-2014-7901, CVE-2014-7902, CVE-2014-7903, CVE-2014-7904, CVE-2014-7905, CVE-2014-7906, CVE-2014-7907, CVE-2014-7908, CVE-2014-7909, CVE-2014-7910

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1626-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00048.html>

SuSE Linux 13.1

i586

chromium-ffmpegsumo-39.0.2171.65-58.4

chromium-ffmpegsumo-debuginfo-39.0.2171.65-58.4

chromium-39.0.2171.65-58.4

chromium-desktop-gnome-39.0.2171.65-58.4

chromium-debuginfo-39.0.2171.65-58.4

chromium-debugsource-39.0.2171.65-58.4

chromedriver-debuginfo-39.0.2171.65-58.4

chromium-desktop-kde-39.0.2171.65-58.4

chromedriver-39.0.2171.65-58.4

SuSE Linux 13.2

i586

chromium-ffmpegsumo-debuginfo-39.0.2171.65-4.4

chromium-debuginfo-39.0.2171.65-4.4

chromium-39.0.2171.65-4.4

chromium-ffmpegsumo-39.0.2171.65-4.4

chromium-desktop-kde-39.0.2171.65-4.4

chromium-debugsource-39.0.2171.65-4.4

chromium-desktop-gnome-39.0.2171.65-4.4

chromedriver-debuginfo-39.0.2171.65-4.4

chromedriver-39.0.2171.65-4.4

### 170437 - Amazon Linux AMI ALAS-2014-461 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9356, CVE-2014-9357, CVE-2014-9358

#### Description

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

ALAS-2014-461

#### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2014-461.html>

Amazon Linux AMI

x86\_64

docker-pkg-devel-1.3.3-1.0.amzn1

docker-devel-1.3.3-1.0.amzn1

docker-1.3.3-1.0.amzn1

### 174611 - Scientific Linux Security ERRATA Important: rpm on SL7.x x86\_64 (1412-1453)

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: rpm on SL7.x x86\_64 (1412-1453)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1453>

SL7

x86\_64

rpm-build-libs-4.11.1-18.el7\_0

rpm-sign-4.11.1-18.el7\_0

rpm-4.11.1-18.el7\_0

rpm-devel-4.11.1-18.el7\_0

rpm-build-4.11.1-18.el7\_0

rpm-debuginfo-4.11.1-18.el7\_0

rpm-python-4.11.1-18.el7\_0

rpm-libs-4.11.1-18.el7\_0

noarch

rpm-cron-4.11.1-18.el7\_0

rpm-apidocs-4.11.1-18.el7\_0

## **178006 - Gentoo Linux GLSA-201412-07 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8439, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-07

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-07.xml>

Affected packages:

www-plugins/adobe-flash < 11.2.202.425

## **178011 - Gentoo Linux GLSA-201412-24 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-1447, CVE-2013-4289, CVE-2013-4290, CVE-2013-6045, CVE-2013-6052, CVE-2013-6053, CVE-2013-6054, CVE-2013-6887

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-24

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-24.xml>

Affected packages:  
media-libs/openjpeg < 1.5.2

### **178012 - Gentoo Linux GLSA-201412-28 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2010-3933, CVE-2011-0446, CVE-2011-0447, CVE-2011-0448, CVE-2011-0449, CVE-2011-2929, CVE-2011-2930, CVE-2011-2931, CVE-2011-2932, CVE-2011-3186, CVE-2013-0155, CVE-2013-0156, CVE-2013-0276, CVE-2013-0277, CVE-2013-0333, CVE-2013-1854, CVE-2013-1855, CVE-2013-1856, CVE-2013-1857

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-28

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-28.xml>

Affected packages:  
dev-ruby/rails < 2.3.18

### **178015 - Gentoo Linux GLSA-201412-09 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2007-4370, CVE-2009-4023, CVE-2009-4111, CVE-2010-0778, CVE-2010-1780, CVE-2010-1782, CVE-2010-1783, CVE-2010-1784, CVE-2010-1785, CVE-2010-1786, CVE-2010-1787, CVE-2010-1788, CVE-2010-1790, CVE-2010-1791, CVE-2010-1792, CVE-2010-1793, CVE-2010-1807, CVE-2010-1812, CVE-2010-1814, CVE-2010-1815, CVE-2010-2526, CVE-2010-2901, CVE-2010-3255, CVE-2010-3257, CVE-2010-3259, CVE-2010-3362, CVE-2010-3374, CVE-2010-3389, CVE-2010-3812, CVE-2010-3813, CVE-2010-3999, CVE-2010-4042, CVE-2010-4197, CVE-2010-4198, CVE-2010-4204, CVE-2010-4206, CVE-2010-4492, CVE-2010-4493, CVE-2010-4577, CVE-2010-4578, CVE-2011-0007, CVE-2011-0465, CVE-2011-0482, CVE-2011-0721, CVE-2011-0727, CVE-2011-0904, CVE-2011-0905, CVE-2011-1072, CVE-2011-1097, CVE-2011-1144, CVE-2011-1425, CVE-2011-1572, CVE-2011-1760, CVE-2011-1951, CVE-2011-2471, CVE-2011-2472, CVE-2011-2473, CVE-2011-2524, CVE-2011-3365, CVE-2011-3366, CVE-2011-3367

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-09

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-09.xml>

Affected packages:  
media-libs/fmod < 4.38.00



dev-php/PEAR-Mail < 1.2.0  
sys-fs/lvm2 < 2.02.72  
app-office/gnucash < 2.4.4  
media-libs/xine-lib < 1.1.19  
media-sound/lastfmplayer < 1.5.4.26862-r3  
net-libs/webkit-gtk < 1.2.7  
sys-apps/shadow < 4.1.4.3  
dev-php/PEAR-PEAR < 1.9.2-r1  
dev-db/unixODBC < 2.3.0-r1  
sys-cluster/resource-agents < 1.0.4-r1  
net-misc/mrouted < 3.9.5  
net-misc/rsync < 3.0.8  
dev-libs/xmlsec < 1.2.17  
x11-apps/xrdb < 1.0.9  
net-misc/vino < 2.32.2  
dev-util/oprofile < 0.9.6-r1  
app-admin/syslog-ng < 3.2.4  
net-analyzer/sflowtool < 3.20  
gnome-base/gdm < 3.8.4-r3  
net-libs/libsoup < 2.34.3  
app-misc/ca-certificates < 20110502-r1  
dev-vcs/gitolite < 1.5.9.1  
dev-util/qt-creator < 2.1.0

## 178019 - Gentoo Linux GLSA-201412-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-3005, CVE-2007-2741, CVE-2008-0553, CVE-2008-1382, CVE-2008-5907, CVE-2008-6218, CVE-2008-6661, CVE-2009-0040, CVE-2009-0360, CVE-2009-0361, CVE-2009-0946, CVE-2009-2042, CVE-2009-2624, CVE-2009-3736, CVE-2009-4029, CVE-2009-4411, CVE-2009-4896, CVE-2010-0001, CVE-2010-0436, CVE-2010-0732, CVE-2010-0829, CVE-2010-1000, CVE-2010-1205, CVE-2010-1511, CVE-2010-2056, CVE-2010-2060, CVE-2010-2192, CVE-2010-2251, CVE-2010-2529, CVE-2010-2809, CVE-2010-2945

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-08

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-08.xml>

Affected packages:

dev-util/insight < 6.7.1-r1  
dev-perl/perl-tk < 804.028-r2  
dev-util/sourcenv < 5.1.4  
dev-lang/tk < 8.4.18-r1  
sys-block/partimage < 0.6.8  
app-antivirus/bitdefender-console <= 7.1  
net-mail/mlmmj < 1.2.17.1  
sys-apps/acl < 2.2.49  
x11-apps/xinit < 1.2.0-r4  
app-arch/gzip < 1.4  
app-arch/ncompress < 4.2.4.3  
dev-libs/liblzw < 0.2  
media-gfx/splashutils < 1.5.4.3-r3

sys-devel/m4 < 1.4.14-r1  
kde-base/kdm < 4.3.5-r1  
x11-libs/gtk+ < 2.18.7  
kde-base/kget < 4.3.5-r1  
app-text/dvipng < 1.13  
app-misc/beanstalkd < 1.4.6  
sys-apps/pmount < 0.9.23  
sys-auth/pam\_krb5 < 4.3  
app-text/gv < 3.7.1  
net-ftp/lftp < 4.0.6  
www-client/uzbl < 2010.08.05  
x11-misc/slim < 1.3.2  
net-misc/iputils < 20100418  
media-tv/dvbstreamer < 1.1-r1

## 178022 - Gentoo Linux GLSA-201412-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3188, CVE-2014-3189, CVE-2014-3190, CVE-2014-3191, CVE-2014-3192, CVE-2014-3193, CVE-2014-3194, CVE-2014-3195, CVE-2014-3197, CVE-2014-3198, CVE-2014-3199, CVE-2014-3200, CVE-2014-7899, CVE-2014-7900, CVE-2014-7901, CVE-2014-7902, CVE-2014-7903, CVE-2014-7904, CVE-2014-7906, CVE-2014-7907, CVE-2014-7908, CVE-2014-7909, CVE-2014-7910

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-13

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-13.xml>

Affected packages:

www-client/chromium < 39.0.2171.65

## 188636 - Fedora Linux 21 FEDORA-2014-16839 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9356, CVE-2014-9357, CVE-2014-9358

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16839

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146224.html>

Fedora Core 21

docker-io-1.4.0-1.fc21

## 17468 - Google Android WAPPushManager Module SQL Injection Vulnerability

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: High

CVE: CVE-2014-8507

### Description

A SQL injection vulnerability is present in some versions of Google Android.

### Observation

Google Android is a popular mobile operating system.

A SQL injection vulnerability is present in some versions of Google Android. The flaw lies in WAPPushManager. Successful exploitation could allow an attacker to launch any activity or service in the remote phone.

## 17525 - (VMSA-2014-0012) VMware vCenter Server Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2014-4209, CVE-2014-4216, CVE-2014-4218, CVE-2014-4219, CVE-2014-4227, CVE-2014-4244, CVE-2014-4252, CVE-2014-4262, CVE-2014-4263, CVE-2014-4265, CVE-2014-4268, CVE-2014-8371

### Description

Multiple vulnerabilities are present in some versions of VMware vCenter Server.

### Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

Multiple vulnerabilities are present in some versions of VMware vCenter Server. The flaws lie in multiple components such as Oracle Java Runtime Environment. Successful exploitation could allow an attacker to execute remote code.

## 17539 - Z-Scada Net Unspecified Defect Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

### Description

A vulnerability in some versions of Z-Scada Net could lead to remote code execution.

### Observation

A vulnerability in some versions of Z-Scada Net could lead to remote code execution.

The flaw is due to an unspecified defect. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 178005 - Gentoo Linux GLSA-201412-17 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0196, CVE-2009-0792, CVE-2009-3743, CVE-2009-4270, CVE-2009-4897, CVE-2010-1628, CVE-2010-2055, CVE-

2010-4054, CVE-2012-4405

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-17

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-17.xml>

Affected packages:

app-text/ghostscript-gpl < 9.10-r2

### **178017 - Gentoo Linux GLSA-201412-11 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2007-0720, CVE-2007-1536, CVE-2007-2026, CVE-2007-2445, CVE-2007-2741, CVE-2007-3108, CVE-2007-4995, CVE-2007-5116, CVE-2007-5135, CVE-2007-5266, CVE-2007-5268, CVE-2007-5269, CVE-2007-5849, CVE-2010-1205, CVE-2013-0338, CVE-2013-0339, CVE-2013-1664, CVE-2013-1969, CVE-2013-2877, CVE-2014-0160

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-11

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-11.xml>

Affected packages:

app-emulation/emul-linux-x86-baselibs < 20140406-r1

### **17466 - Google Android Settings Application Privilege Escalation Vulnerability**

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: High

CVE: CVE-2014-8609

#### Description

A privilege escalation vulnerability is present in some versions of Google Android.

#### Observation

Google Android is a popular mobile operating system.

A privilege escalation vulnerability is present in some versions of Google Android. The flaw lies in Android Settings application. Successful exploitation could allow a local app to broadcast sensitive intent with the permission of SYSTEM.

### **17546 - Honeywell OPOS Suite Open Method Remote Code Execution**

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-8269

#### Description

A vulnerability in some versions of Honeywell OPOS Suite could lead to remote code execution.

#### Observation

A vulnerability in some versions of Honeywell OPOS Suite could lead to remote code execution.

The flaw lies in HWOPOSScale.ocx and HWOPOSSCANNER.ocx. Successful exploitation by a remote attacker could result in the execution of arbitrary code or a denial of service.

### 91687 - Oracle Enterprise Linux ELSA-2014-1984 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-1033, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2014-8500

#### Description

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

ELSA-2014-1984

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2014-December/004725.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004724.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004722.html>

#### OEL6

x86\_64

bind-9.8.2-0.30.rc1.el6\_6.1

bind-chroot-9.8.2-0.30.rc1.el6\_6.1

bind-devel-9.8.2-0.30.rc1.el6\_6.1

bind-utils-9.8.2-0.30.rc1.el6\_6.1

bind-libs-9.8.2-0.30.rc1.el6\_6.1

bind-sdb-9.8.2-0.30.rc1.el6\_6.1

#### i386

bind-9.8.2-0.30.rc1.el6\_6.1

bind-chroot-9.8.2-0.30.rc1.el6\_6.1

bind-devel-9.8.2-0.30.rc1.el6\_6.1

bind-utils-9.8.2-0.30.rc1.el6\_6.1

bind-libs-9.8.2-0.30.rc1.el6\_6.1

bind-sdb-9.8.2-0.30.rc1.el6\_6.1

#### OEL5

x86\_64

bind-libs-9.3.6-25.P1.el5\_11.2

bind-devel-9.3.6-25.P1.el5\_11.2

bind-chroot-9.3.6-25.P1.el5\_11.2

bind-libbind-devel-9.3.6-25.P1.el5\_11.2

bind-sdb-9.3.6-25.P1.el5\_11.2

caching-nameserver-9.3.6-25.P1.el5\_11.2

bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

i386

bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

OEL7

x86\_64  
bind-license-9.9.4-14.0.1.el7\_0.1  
bind-lite-devel-9.9.4-14.0.1.el7\_0.1  
bind-chroot-9.9.4-14.0.1.el7\_0.1  
bind-libs-lite-9.9.4-14.0.1.el7\_0.1  
bind-sdb-9.9.4-14.0.1.el7\_0.1  
bind-sdb-chroot-9.9.4-14.0.1.el7\_0.1  
bind-utils-9.9.4-14.0.1.el7\_0.1  
bind-9.9.4-14.0.1.el7\_0.1  
bind-devel-9.9.4-14.0.1.el7\_0.1  
bind-libs-9.9.4-14.0.1.el7\_0.1

## 188672 - Fedora Linux 20 FEDORA-2014-16003 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4287, CVE-2014-6463, CVE-2014-6464, CVE-2014-6469, CVE-2014-6484, CVE-2014-6505, CVE-2014-6507, CVE-2014-6520, CVE-2014-6530, CVE-2014-6551, CVE-2014-6555, CVE-2014-6559, CVE-2014-6564

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16003

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145916.html>

Fedora Core 20

mariadb-5.5.40-1.fc20

## 17337 - (HPSBUX03162) HP-UX OpenSSL Multiple Vulnerabilities

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

Risk Level: High

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

### Description

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

## Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in OpenSSL component. Successful exploitation could allow an attacker to cause denial of service, obtain unauthorized access, or launch a man-in-the-middle attack.

## **85840 - CentOS 5 CESA-2014-1985 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8500

## Description

The scan detected that the host is missing the following update:  
CESA-2014-1985

## Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020826.html>

CentOS 5

x86\_64

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

i386

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

## **85844 - CentOS 5, 6, 7 CESA-2014-1984 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8500

## Description

The scan detected that the host is missing the following update:  
CESA-2014-1984

## Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020828.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020829.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020827.html>

## CentOS 7

x86\_64

bind-libs-9.9.4-14.el7\_0.1  
bind-chroot-9.9.4-14.el7\_0.1  
bind-sdb-9.9.4-14.el7\_0.1  
bind-9.9.4-14.el7\_0.1  
bind-lite-devel-9.9.4-14.el7\_0.1  
bind-devel-9.9.4-14.el7\_0.1  
bind-utils-9.9.4-14.el7\_0.1  
bind-libs-lite-9.9.4-14.el7\_0.1  
bind-sdb-chroot-9.9.4-14.el7\_0.1

i686

bind-lite-devel-9.9.4-14.el7\_0.1  
bind-libs-9.9.4-14.el7\_0.1  
bind-devel-9.9.4-14.el7\_0.1  
bind-libs-lite-9.9.4-14.el7\_0.1

noarch

bind-license-9.9.4-14.el7\_0.1

## CentOS 5

x86\_64

bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

i386

bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

## CentOS 6

x86\_64

bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-devel-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-sdb-9.8.2-0.30.rc1.el6\_6.1

i686

bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-devel-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-sdb-9.8.2-0.30.rc1.el6\_6.1



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

Risk Level: High

CVE: CVE-2013-2929, CVE-2014-1739, CVE-2014-3181, CVE-2014-3182, CVE-2014-3184, CVE-2014-3185, CVE-2014-3186, CVE-2014-3631, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4654, CVE-2014-4655, CVE-2014-4656, CVE-2014-5045, CVE-2014-6410

#### Description

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

CESA-2014-1971

#### Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2014-December/020820.html>

CentOS 7

x86\_64

perf-3.10.0-123.13.1.el7

kernel-tools-3.10.0-123.13.1.el7

kernel-tools-libs-3.10.0-123.13.1.el7

kernel-3.10.0-123.13.1.el7

kernel-devel-3.10.0-123.13.1.el7

kernel-debug-devel-3.10.0-123.13.1.el7

kernel-debug-3.10.0-123.13.1.el7

kernel-headers-3.10.0-123.13.1.el7

kernel-tools-libs-devel-3.10.0-123.13.1.el7

python-perf-3.10.0-123.13.1.el7

noarch

kernel-abi-whitelists-3.10.0-123.13.1.el7

kernel-doc-3.10.0-123.13.1.el7

### 88656 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-344-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

#### Description

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

SSA:2014-344-01

#### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.511270>

Slackware 13.0

x86\_64

bind-9.9.6\_P1-x86\_64-1

Slackware 14.1

x86\_64

bind-9.9.6\_P1-x86\_64-1

Slackware 13.37  
x86\_64  
bind-9.9.6\_P1-x86\_64-1

Slackware 13.1  
x86\_64  
bind-9.9.6\_P1-x86\_64-1

Slackware 14.0  
x86\_64  
bind-9.9.6\_P1-x86\_64-1

## 91688 - Oracle Enterprise Linux ELSA-2014-1971 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2929, CVE-2014-1739, CVE-2014-3181, CVE-2014-3182, CVE-2014-3184, CVE-2014-3185, CVE-2014-3186, CVE-2014-3611, CVE-2014-3631, CVE-2014-3645, CVE-2014-3646, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4654, CVE-2014-4655, CVE-2014-4656, CVE-2014-5045, CVE-2014-6410

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1971

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004709.html>

OEL7  
x86\_64  
kernel-tools-libs-devel-3.10.0-123.13.1.el7  
perf-3.10.0-123.13.1.el7  
kernel-tools-3.10.0-123.13.1.el7  
kernel-tools-libs-3.10.0-123.13.1.el7  
kernel-3.10.0-123.13.1.el7  
kernel-headers-3.10.0-123.13.1.el7  
kernel-debug-devel-3.10.0-123.13.1.el7  
kernel-debug-3.10.0-123.13.1.el7  
kernel-devel-3.10.0-123.13.1.el7  
kernel-doc-3.10.0-123.13.1.el7  
kernel-abi-whitelists-3.10.0-123.13.1.el7  
python-perf-3.10.0-123.13.1.el7

## 91690 - Oracle Enterprise Linux ELSA-2014-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1985

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004723.html>

#### OEL5

x86\_64

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

#### i386

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

## 93432 - Mandriva Linux MBS1 MDVSA-2014-249 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7840, CVE-2014-8106

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-249

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A249/>

Mandriva Linux mbs1

x86\_64

qemu-img-1.6.2-1.2

qemu-1.6.2-1.2

## 93433 - Mandriva Linux MBS1 MDVSA-2014-239 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-239

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A239/>

Mandriva Linux mbs1  
x86\_64  
lib64flac8-1.2.1-11.1  
lib64flac++6-1.2.1-11.1  
lib64flac-devel-1.2.1-11.1  
flac-1.2.1-11.1  
lib64flac++-devel-1.2.1-11.1

### 93435 - Mandriva Linux MBS1 MDVSA-2014-248 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

#### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-248

#### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A248/>

Mandriva Linux mbs1  
x86\_64  
lib64gvc6-2.28.0-6.2  
lua-graphviz-2.28.0-6.2  
php-graphviz-2.28.0-6.2  
ruby-graphviz-2.28.0-6.2  
java-graphviz-2.28.0-6.2  
graphviz-doc-2.28.0-6.2  
lib64graphviz-static-devel-2.28.0-6.2  
lib64cgraph6-2.28.0-6.2  
lib64xdot4-2.28.0-6.2  
graphviz-2.28.0-6.2  
perl-graphviz-2.28.0-6.2  
python-graphviz-2.28.0-6.2  
lib64cdt5-2.28.0-6.2  
tcl-graphviz-2.28.0-6.2  
lib64pathplan4-2.28.0-6.2  
lib64graph5-2.28.0-6.2  
lib64graphviz-devel-2.28.0-6.2  
lib64gvpr2-2.28.0-6.2  
ocaml-graphviz-2.28.0-6.2

### 93436 - Mandriva Linux MBS1 MDVSA-2014-238 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

#### Description

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

MDVSA-2014-238

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A238/>

Mandriva Linux mbs1  
x86\_64  
bind-utils-9.9.6.p1-1  
bind-devel-9.9.6.p1-1  
bind-9.9.6.p1-1  
bind-doc-9.9.6.p1-1  
bind-sdb-9.9.6.p1-1

## 93439 - Mandriva Linux MBS1 MDVSA-2014-244 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1794, CVE-2013-1795, CVE-2013-4134, CVE-2013-4135, CVE-2014-0159, CVE-2014-3660

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-244

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A244/>

Mandriva Linux mbs1  
x86\_64  
openafs-doc-1.4.15-1.1  
openafs-client-1.4.15-1.1  
openafs-server-1.4.15-1.1  
openafs-1.4.15-1.1  
lib64openafs-devel-1.4.15-1.1  
dkms-libafs-1.4.15-1.1  
lib64openafs1-1.4.15-1.1

## 93442 - Mandriva Linux MBS1 MDVSA-2014-252 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1569, CVE-2014-3566

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-252

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A252/>

Mandriva Linux mbs1  
x86\_64  
rootcerts-java-20141117.00-1  
lib64nss-static-devel-3.17.3-1  
nss-3.17.3-1  
lib64nss-devel-3.17.3-1  
lib64nss3-3.17.3-1  
rootcerts-20141117.00-1  
nss-doc-3.17.3-1

### 93443 - Mandriva Linux MBS1 MDVSA-2014-247 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9029

#### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-247

#### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A247/>

Mandriva Linux mbs1  
x86\_64  
jasper-1.900.1-14.1  
lib64jasper-devel-1.900.1-14.1  
lib64jasper1-1.900.1-14.1  
lib64jasper-static-devel-1.900.1-14.1

### 130025 - Debian Linux 7.0 DSA-3098-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9157

#### Description

The scan detected that the host is missing the following update:  
DSA-3098-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3098>

Debian 7.0  
all  
graphviz\_2.26.3-14+deb7u2

## 140639 - Red Hat Enterprise Linux RHSA-2014-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

### Description

The scan detected that the host is missing the following update:  
RHSA-2014-1985

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1985.html>

#### RHEL5D

x86\_64

bind97-debuginfo-9.7.0-21.P2.el5\_11.1

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

i386

bind97-debuginfo-9.7.0-21.P2.el5\_11.1

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

#### RHEL5S

x86\_64

bind97-debuginfo-9.7.0-21.P2.el5\_11.1

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

i386

bind97-debuginfo-9.7.0-21.P2.el5\_11.1

bind97-devel-9.7.0-21.P2.el5\_11.1

bind97-chroot-9.7.0-21.P2.el5\_11.1

bind97-utils-9.7.0-21.P2.el5\_11.1

bind97-libs-9.7.0-21.P2.el5\_11.1

bind97-9.7.0-21.P2.el5\_11.1

## 140641 - Red Hat Enterprise Linux RHSA-2014-1997 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6657, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-5471, CVE-2014-5472, CVE-2014-6410, CVE-2014-9322

## Description

The scan detected that the host is missing the following update:  
RHSA-2014-1997

## Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1997.html>

### RHEL6D

x86\_64  
kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6  
perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6  
kernel-debuginfo-common-x86\_64-2.6.32-504.3.3.el6

### i386

kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6  
perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-common-i686-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6

### noarch

kernel-abi-whitelists-2.6.32-504.3.3.el6  
kernel-doc-2.6.32-504.3.3.el6  
kernel-firmware-2.6.32-504.3.3.el6

### RHEL6S

x86\_64  
kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6  
perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6  
kernel-debuginfo-common-x86\_64-2.6.32-504.3.3.el6

### i386

kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6



perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-common-i686-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6

noarch  
kernel-abi-whitelists-2.6.32-504.3.3.el6  
kernel-doc-2.6.32-504.3.3.el6  
kernel-firmware-2.6.32-504.3.3.el6

#### RHEL6WS

x86\_64  
kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6  
perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6  
kernel-debuginfo-common-x86\_64-2.6.32-504.3.3.el6

i386  
kernel-debug-devel-2.6.32-504.3.3.el6  
perf-2.6.32-504.3.3.el6  
perf-debuginfo-2.6.32-504.3.3.el6  
python-perf-debuginfo-2.6.32-504.3.3.el6  
kernel-debug-2.6.32-504.3.3.el6  
kernel-debuginfo-common-i686-2.6.32-504.3.3.el6  
kernel-debuginfo-2.6.32-504.3.3.el6  
kernel-2.6.32-504.3.3.el6  
kernel-devel-2.6.32-504.3.3.el6  
kernel-headers-2.6.32-504.3.3.el6  
kernel-debug-debuginfo-2.6.32-504.3.3.el6

noarch  
kernel-abi-whitelists-2.6.32-504.3.3.el6  
kernel-doc-2.6.32-504.3.3.el6  
kernel-firmware-2.6.32-504.3.3.el6

### 140643 - Red Hat Enterprise Linux RHSA-2014-1984 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

#### Description

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

RHSA-2014-1984

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1984.html>

#### RHEL5D

x86\_64

bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
bind-libs-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

i386

bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
bind-libs-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

#### RHEL5S

x86\_64

bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

i386

bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

#### RHEL7S

x86\_64

bind-9.9.4-14.el7\_0.1  
bind-debuginfo-9.9.4-14.el7\_0.1  
bind-utils-9.9.4-14.el7\_0.1  
bind-libs-lite-9.9.4-14.el7\_0.1  
bind-libs-9.9.4-14.el7\_0.1  
bind-chroot-9.9.4-14.el7\_0.1

noarch

bind-license-9.9.4-14.el7\_0.1

#### RHEL6S

x86\_64

bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1

bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

i386  
bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

RHEL7D  
x86\_64  
bind-debuginfo-9.9.4-14.el7\_0.1  
bind-utils-9.9.4-14.el7\_0.1  
bind-libs-9.9.4-14.el7\_0.1  
bind-libs-lite-9.9.4-14.el7\_0.1

noarch  
bind-license-9.9.4-14.el7\_0.1

RHEL6D  
x86\_64  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

i386  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

RHEL6WS  
x86\_64  
bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

i386  
bind-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

RHEL7WS  
x86\_64  
bind-9.9.4-14.el7\_0.1  
bind-debuginfo-9.9.4-14.el7\_0.1  
bind-utils-9.9.4-14.el7\_0.1  
bind-libs-lite-9.9.4-14.el7\_0.1  
bind-libs-9.9.4-14.el7\_0.1  
bind-chroot-9.9.4-14.el7\_0.1

noarch  
bind-license-9.9.4-14.el7\_0.1

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

Risk Level: High

CVE: CVE-2014-8120

### Description

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

RHSA-2014-2000

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2014-2000.html>

RHEL7WS

x86\_64

thermostat1-thermostat-1.0.4-70.6.el7

thermostat1-thermostat-debuginfo-1.0.4-70.6.el7

noarch

thermostat1-thermostat-javadoc-1.0.4-70.6.el7

thermostat1-thermostat-webapp-1.0.4-70.6.el7

RHEL7S

x86\_64

thermostat1-thermostat-1.0.4-70.6.el7

thermostat1-thermostat-debuginfo-1.0.4-70.6.el7

noarch

thermostat1-thermostat-javadoc-1.0.4-70.6.el7

thermostat1-thermostat-webapp-1.0.4-70.6.el7

RHEL6S

x86\_64

thermostat1-thermostat-debuginfo-1.0.4-60.6.el6

thermostat1-thermostat-1.0.4-60.6.el6

noarch

thermostat1-thermostat-javadoc-1.0.4-60.6.el6

thermostat1-thermostat-webapp-1.0.4-60.6.el6

RHEL6WS

x86\_64

thermostat1-thermostat-debuginfo-1.0.4-60.6.el6

thermostat1-thermostat-1.0.4-60.6.el6

noarch

thermostat1-thermostat-javadoc-1.0.4-60.6.el6

thermostat1-thermostat-webapp-1.0.4-60.6.el6

## 142561 - SuSE SLES 11 SP3, SLED 11 SP3 shim-2014-11-20-9997 Update Is Not Installed

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

Risk Level: High

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

### Description

The scan detected that the host is missing the following update:  
shim-2014-11-20-9997

#### Observation

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

<https://download.suse.com/Download?buildid=iLZ9FPcA0OI~>  
[https://download.suse.com/Download?buildid=FI9ckURc\\_Ag~](https://download.suse.com/Download?buildid=FI9ckURc_Ag~)  
<https://download.suse.com/Download?buildid=y64c3OfPVD0~>

SuSE SLED 11 SP3  
x86\_64  
shim-0.7.318.81ee561d-0.9.2

SuSE SLES 11 SP3  
x86\_64  
gnu-efi-3.0u-0.7.2  
shim-0.7.318.81ee561d-0.9.2

### 142573 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1644-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9029

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1644-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00062.html>

SuSE Linux 13.1  
x86\_64  
libjasper1-32bit-1.900.1-160.5.1  
libjasper1-debuginfo-32bit-1.900.1-160.5.1

i586  
libjasper-devel-1.900.1-160.5.1  
jasper-debuginfo-1.900.1-160.5.1  
libjasper1-1.900.1-160.5.1  
libjasper1-debuginfo-1.900.1-160.5.1  
jasper-debugsource-1.900.1-160.5.1  
jasper-1.900.1-160.5.1

SuSE Linux 12.3  
x86\_64  
libjasper1-debuginfo-32bit-1.900.1-156.5.1  
libjasper1-32bit-1.900.1-156.5.1

i586  
libjasper1-1.900.1-156.5.1  
jasper-debuginfo-1.900.1-156.5.1

libjasper1-debuginfo-1.900.1-156.5.1  
jasper-debugsource-1.900.1-156.5.1  
libjasper-devel-1.900.1-156.5.1  
jasper-1.900.1-156.5.1

SuSE Linux 13.2

x86\_64

libjasper1-32bit-1.900.1-163.5.1

libjasper1-debuginfo-32bit-1.900.1-163.5.1

i586

libjasper1-1.900.1-163.5.1

libjasper-devel-1.900.1-163.5.1

jasper-1.900.1-163.5.1

jasper-debugsource-1.900.1-163.5.1

jasper-debuginfo-1.900.1-163.5.1

libjasper1-debuginfo-1.900.1-163.5.1

## 174607 - Scientific Linux Security ERRATA Important: bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-2229)

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

Risk Level: High

CVE: CVE-2014-8500

### Description

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

Security ERRATA Important: bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-2229)

### Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=2229>

SL7

x86\_64

bind-libs-9.9.4-14.el7\_0.1

bind-chroot-9.9.4-14.el7\_0.1

bind-sdb-9.9.4-14.el7\_0.1

bind-lite-devel-9.9.4-14.el7\_0.1

bind-debuginfo-9.9.4-14.el7\_0.1

bind-9.9.4-14.el7\_0.1

bind-devel-9.9.4-14.el7\_0.1

bind-utils-9.9.4-14.el7\_0.1

bind-libs-lite-9.9.4-14.el7\_0.1

bind-sdb-chroot-9.9.4-14.el7\_0.1

noarch

bind-license-9.9.4-14.el7\_0.1

SL6

x86\_64

bind-utils-9.8.2-0.30.rc1.el6\_6.1

bind-chroot-9.8.2-0.30.rc1.el6\_6.1

bind-devel-9.8.2-0.30.rc1.el6\_6.1

bind-sdb-9.8.2-0.30.rc1.el6\_6.1

bind-libs-9.8.2-0.30.rc1.el6\_6.1

bind-9.8.2-0.30.rc1.el6\_6.1

bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

i386

bind-utils-9.8.2-0.30.rc1.el6\_6.1  
bind-chroot-9.8.2-0.30.rc1.el6\_6.1  
bind-devel-9.8.2-0.30.rc1.el6\_6.1  
bind-sdb-9.8.2-0.30.rc1.el6\_6.1  
bind-libs-9.8.2-0.30.rc1.el6\_6.1  
bind-9.8.2-0.30.rc1.el6\_6.1  
bind-debuginfo-9.8.2-0.30.rc1.el6\_6.1

SL5

x86\_64  
bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

i386

bind-libbind-devel-9.3.6-25.P1.el5\_11.2  
bind-libs-9.3.6-25.P1.el5\_11.2  
bind-devel-9.3.6-25.P1.el5\_11.2  
bind-chroot-9.3.6-25.P1.el5\_11.2  
bind-sdb-9.3.6-25.P1.el5\_11.2  
caching-nameserver-9.3.6-25.P1.el5\_11.2  
bind-debuginfo-9.3.6-25.P1.el5\_11.2  
bind-utils-9.3.6-25.P1.el5\_11.2  
bind-9.3.6-25.P1.el5\_11.2

## 174609 - Scientific Linux Security ERRATA Important: rpm on SL5.x, SL6.x i386/x86\_64 (1412-1571)

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

Risk Level: High

CVE: CVE-2013-6435

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: rpm on SL5.x, SL6.x i386/x86\_64 (1412-1571)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1571>

SL6

x86\_64  
rpm-python-4.8.0-38.el6\_6  
rpm-4.8.0-38.el6\_6  
rpm-debuginfo-4.8.0-38.el6\_6  
rpm-build-4.8.0-38.el6\_6  
rpm-devel-4.8.0-38.el6\_6  
rpm-libs-4.8.0-38.el6\_6

i386  
rpm-python-4.8.0-38.el6\_6  
rpm-4.8.0-38.el6\_6  
rpm-debuginfo-4.8.0-38.el6\_6  
rpm-build-4.8.0-38.el6\_6  
rpm-devel-4.8.0-38.el6\_6  
rpm-libs-4.8.0-38.el6\_6

noarch  
rpm-apidocs-4.8.0-38.el6\_6  
rpm-cron-4.8.0-38.el6\_6

SL5  
x86\_64  
rpm-devel-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-apidocs-4.4.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11  
rpm-build-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-python-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11

i386  
rpm-devel-4.4.2.3-36.el5\_11  
rpm-4.4.2.3-36.el5\_11  
rpm-apidocs-4.4.2.3-36.el5\_11  
rpm-debuginfo-4.4.2.3-36.el5\_11  
rpm-build-4.4.2.3-36.el5\_11  
popt-1.10.2.3-36.el5\_11  
rpm-python-4.4.2.3-36.el5\_11  
rpm-libs-4.4.2.3-36.el5\_11

## 174610 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86\_64 (1412-1701)

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

Risk Level: High

CVE: CVE-2013-2929, CVE-2014-1739, CVE-2014-3181, CVE-2014-3182, CVE-2014-3184, CVE-2014-3185, CVE-2014-3186, CVE-2014-3631, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4654, CVE-2014-4655, CVE-2014-4656, CVE-2014-5045, CVE-2014-6410

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: kernel on SL7.x x86\_64 (1412-1701)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1701>

SL7  
x86\_64  
kernel-debuginfo-3.10.0-123.13.1.el7  
kernel-tools-debuginfo-3.10.0-123.13.1.el7  
perf-3.10.0-123.13.1.el7  
kernel-tools-3.10.0-123.13.1.el7  
kernel-debuginfo-common-x86\_64-3.10.0-123.13.1.el7



kernel-debug-debuginfo-3.10.0-123.13.1.el7  
kernel-3.10.0-123.13.1.el7  
kernel-devel-3.10.0-123.13.1.el7  
kernel-debug-devel-3.10.0-123.13.1.el7  
kernel-debug-3.10.0-123.13.1.el7  
kernel-tools-libs-devel-3.10.0-123.13.1.el7  
python-perf-debuginfo-3.10.0-123.13.1.el7  
kernel-headers-3.10.0-123.13.1.el7  
kernel-tools-libs-3.10.0-123.13.1.el7  
python-perf-3.10.0-123.13.1.el7  
perf-debuginfo-3.10.0-123.13.1.el7

noarch  
kernel-abi-whitelists-3.10.0-123.13.1.el7  
kernel-doc-3.10.0-123.13.1.el7

## 174612 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86\_64 (1412-2102)

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

Risk Level: High

CVE: CVE-2014-8500

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: bind97 on SL5.x i386/x86\_64 (1412-2102)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=2102>

SL5  
x86\_64  
bind97-debuginfo-9.7.0-21.P2.el5\_11.1  
bind97-devel-9.7.0-21.P2.el5\_11.1  
bind97-chroot-9.7.0-21.P2.el5\_11.1  
bind97-utils-9.7.0-21.P2.el5\_11.1  
bind97-libs-9.7.0-21.P2.el5\_11.1  
bind97-9.7.0-21.P2.el5\_11.1

i386  
bind97-debuginfo-9.7.0-21.P2.el5\_11.1  
bind97-devel-9.7.0-21.P2.el5\_11.1  
bind97-chroot-9.7.0-21.P2.el5\_11.1  
bind97-utils-9.7.0-21.P2.el5\_11.1  
bind97-libs-9.7.0-21.P2.el5\_11.1  
bind97-9.7.0-21.P2.el5\_11.1

## 178002 - Gentoo Linux GLSA-201412-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-4776, CVE-2010-2713, CVE-2010-3313, CVE-2010-3314, CVE-2011-0765, CVE-2011-2198, CVE-2012-0807, CVE-2012-0808, CVE-2012-1620, CVE-2012-2738, CVE-2012-3448

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-10

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-10.xml>

Affected packages:

www-apps/egroupware < 1.8.004.20120613

x11-libs/vte < 0.32.2

net-analyzer/lft < 3.33

dev-php/suhosin < 0.9.33

x11-misc/slock < 1.0

sys-cluster/ganglia < 3.3.7

net-im/gg-transport < 2.2.4

### **178007 - Gentoo Linux GLSA-201412-27 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-0188, CVE-2011-1004, CVE-2011-1005, CVE-2011-4815, CVE-2012-4481, CVE-2012-5371, CVE-2013-0269, CVE-2013-1821, CVE-2013-4164, CVE-2014-8080, CVE-2014-8090

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-27

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-27.xml>

Affected packages:

dev-lang/ruby < 2.0.0\_p598

### **178010 - Gentoo Linux GLSA-201412-18 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-0250

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-18

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-18.xml>

Affected packages:

net-misc/freerdp < 1.1.0\_beta1

### 178021 - Gentoo Linux GLSA-201412-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3158

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-19

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-19.xml>

Affected packages:  
net-dialup/ppp < 2.4.7

### 178025 - Gentoo Linux GLSA-201412-23 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6096, CVE-2013-7108, CVE-2013-7205

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-23

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-23.xml>

Affected packages:  
net-analyzer/nagios-core < 3.5.1

### 181303 - FreeBSD bind Denial Of Service Vulnerability (ab3e98d9-8175-11e4-907d-d050992ecde8)

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2014-8680

#### Description

The scan detected that the host is missing the following update:  
bind -- denial of service vulnerability (ab3e98d9-8175-11e4-907d-d050992ecde8)

#### Observation

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

<http://www.vuxml.org/freebsd/ab3e98d9-8175-11e4-907d-d050992ecde8.html>

Affected packages:

bind99 < 9.9.6  
bind99-base < 9.9.6  
9.3 < FreeBSD < 9.3\_6  
9.2 < FreeBSD < 9.2\_16  
9.1 < FreeBSD < 9.1\_23  
8.4 < FreeBSD < 8.4\_20

**181305 - FreeBSD NVIDIA UNIX driver Remote Denial Of Service Or Arbitrary Code Execution (fdf72a0e-8371-11e4-bc20-001636d274f3)**

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

Risk Level: High

CVE: CVE-2014-8093, CVE-2014-8098, CVE-2014-8298

Description

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

NVIDIA UNIX driver -- remote denial of service or arbitrary code execution (fdf72a0e-8371-11e4-bc20-001636d274f3)

Observation

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

For more information see:

<http://www.vuxml.org/freebsd/fdf72a0e-8371-11e4-bc20-001636d274f3.html>

Affected packages:

nvidia-driver < 340.65  
nvidia-driver-304 < 304.125  
nvidia-driver-173 <= 173.14.35\_3  
nvidia-driver-96 <= 96.43.23\_2  
nvidia-driver-71 <= 71.86.15\_4

**184643 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2438-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8091, CVE-2014-8098, CVE-2014-8298

Description

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

USN-2438-1

Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002759.html>

Ubuntu 14.10

nvidia-331-updates\_331.113-0ubuntu0.1  
nvidia-304\_304.125-0ubuntu0.1  
nvidia-331\_331.113-0ubuntu0.1  
nvidia-304-updates\_304.125-0ubuntu0.1

Ubuntu 14.04

nvidia-331\_331.113-0ubuntu0.0.4  
nvidia-304\_304.125-0ubuntu0.0.1  
nvidia-304-updates\_304.125-0ubuntu0.0.1  
nvidia-331-updates\_331.113-0ubuntu0.0.4

Ubuntu 12.04

nvidia-331\_331.113-0ubuntu0.0.0.3  
nvidia-304\_304.125-0ubuntu0.0.0.1  
nvidia-331-updates\_331.113-0ubuntu0.0.0.3  
nvidia-304-updates\_304.125-0ubuntu0.0.0.1

### 184645 - Ubuntu Linux 10.04 USN-2442-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7841, CVE-2014-8134, CVE-2014-8709, CVE-2014-8884, CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
USN-2442-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002763.html>

Ubuntu 10.04

linux-image-2.6.32-374-ec2\_2.6.32-374.91

### 184647 - Ubuntu Linux 14.04 USN-2446-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7825, CVE-2014-7826, CVE-2014-8134, CVE-2014-8369, CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
USN-2446-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002767.html>

Ubuntu 14.04

linux-image-3.13.0-43-powerpc-e500mc\_3.13.0-43.72

linux-image-3.13.0-43-powerpc-smp\_3.13.0-43.72  
linux-image-3.13.0-43-powerpc-e500\_3.13.0-43.72  
linux-image-3.13.0-43-powerpc64-smp\_3.13.0-43.72  
linux-image-3.13.0-43-generic\_3.13.0-43.72  
linux-image-3.13.0-43-powerpc64-emb\_3.13.0-43.72  
linux-image-3.13.0-43-lowlatency\_3.13.0-43.72  
linux-image-3.13.0-43-generic-ipae\_3.13.0-43.72

#### 184648 - Ubuntu Linux 14.10 USN-2448-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7825, CVE-2014-7826, CVE-2014-7970, CVE-2014-8086, CVE-2014-8134, CVE-2014-8369, CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
USN-2448-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002769.html>

Ubuntu 14.10

linux-image-3.16.0-28-generic\_3.16.0-28.37  
linux-image-3.16.0-28-powerpc-smp\_3.16.0-28.37  
linux-image-3.16.0-28-powerpc64-smp\_3.16.0-28.37  
linux-image-3.16.0-28-powerpc64-emb\_3.16.0-28.37  
linux-image-3.16.0-28-lowlatency\_3.16.0-28.37  
linux-image-3.16.0-28-powerpc-e500mc\_3.16.0-28.37  
linux-image-3.16.0-28-generic-ipae\_3.16.0-28.37

#### 184649 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2439-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7840, CVE-2014-8106

#### Description

The scan detected that the host is missing the following update:  
USN-2439-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002760.html>

Ubuntu 14.10

qemu-system-aarch64\_2.1+dfsg-4ubuntu6.3  
qemu-system-arm\_2.1+dfsg-4ubuntu6.3  
qemu-system-sparc\_2.1+dfsg-4ubuntu6.3

qemu-system\_2.1+dfsg-4ubuntu6.3  
qemu-system-misc\_2.1+dfsg-4ubuntu6.3  
qemu-system-mips\_2.1+dfsg-4ubuntu6.3  
qemu-system-x86\_2.1+dfsg-4ubuntu6.3  
qemu-system-ppc\_2.1+dfsg-4ubuntu6.3

Ubuntu 14.04

qemu-system\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-x86\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-sparc\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-misc\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-mips\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-arm\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-ppc\_2.0.0+dfsg-2ubuntu1.9  
qemu-system-aarch64\_2.0.0+dfsg-2ubuntu1.9

Ubuntu 12.04

qemu-kvm\_1.0+noroms-0ubuntu14.21

Ubuntu 10.04

qemu-kvm\_0.12.3+noroms-0ubuntu9.26

## 184650 - Ubuntu Linux 10.04 USN-2441-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7841, CVE-2014-8134, CVE-2014-8709, CVE-2014-8884, CVE-2014-9090

### Description

The scan detected that the host is missing the following update:  
USN-2441-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002762.html>

Ubuntu 10.04

linux-image-2.6.32-70-powerpc64-smp\_2.6.32-70.137  
linux-image-2.6.32-70-386\_2.6.32-70.137  
linux-image-2.6.32-70-server\_2.6.32-70.137  
linux-image-2.6.32-70-sparc64-smp\_2.6.32-70.137  
linux-image-2.6.32-70-generic\_2.6.32-70.137  
linux-image-2.6.32-70-ia64\_2.6.32-70.137  
linux-image-2.6.32-70-virtual\_2.6.32-70.137  
linux-image-2.6.32-70-lpia\_2.6.32-70.137  
linux-image-2.6.32-70-preempt\_2.6.32-70.137  
linux-image-2.6.32-70-generic-pae\_2.6.32-70.137  
linux-image-2.6.32-70-powerpc-smp\_2.6.32-70.137  
linux-image-2.6.32-70-sparc64\_2.6.32-70.137  
linux-image-2.6.32-70-powerpc\_2.6.32-70.137  
linux-image-2.6.32-70-versatile\_2.6.32-70.137

## 184652 - Ubuntu Linux 12.04 USN-2445-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7825, CVE-2014-7826, CVE-2014-8134, CVE-2014-8369, CVE-2014-9090

### Description

The scan detected that the host is missing the following update:  
USN-2445-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002766.html>

Ubuntu 12.04

linux-image-3.13.0-43-generic\_3.13.0-43.72~precise1  
linux-image-3.13.0-43-generic-lpae\_3.13.0-43.72~precise1

## 184653 - Ubuntu Linux 14.04 USN-2447-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-7825, CVE-2014-7826, CVE-2014-7970, CVE-2014-8086, CVE-2014-8134, CVE-2014-8369, CVE-2014-9090

### Description

The scan detected that the host is missing the following update:  
USN-2447-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002768.html>

Ubuntu 14.04

linux-image-3.16.0-28-lowlatency\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-powerpc64-emb\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-powerpc-smp\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-powerpc-e500mc\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-generic-lpae\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-generic\_3.16.0-28.37~14.04.1  
linux-image-3.16.0-28-powerpc64-smp\_3.16.0-28.37~14.04.1

## 188614 - Fedora Linux 20 FEDORA-2014-16270 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028



### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16270

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146154.html>

Fedora Core 20

mingw-flac-1.3.1-1.fc20

## **188620 - Fedora Linux 20 FEDORA-2014-16033 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-6451, CVE-2013-6452, CVE-2013-6453, CVE-2013-6454, CVE-2013-6472, CVE-2014-1610, CVE-2014-2853

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16033

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145969.html>

Fedora Core 20

mediawiki-1.23.7-1.fc20

## **188621 - Fedora Linux 21 FEDORA-2014-16175 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16175

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146056.html>

Fedora Core 21

flac-1.3.1-1.fc21

## 188622 - Fedora Linux 21 FEDORA-2014-16075 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7840

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16075

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145918.html>

Fedora Core 21

qemu-2.1.2-7.fc21

## 188631 - Fedora Linux 19 FEDORA-2014-16020 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6451, CVE-2013-6452, CVE-2013-6453, CVE-2013-6454, CVE-2013-6472, CVE-2014-1610, CVE-2014-2853

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16020

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145910.html>

Fedora Core 19

mediawiki-1.23.7-1.fc19

## 188633 - Fedora Linux 20 FEDORA-2014-16393 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7338, CVE-2014-2667

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16393

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145903.html>

Fedora Core 20

python3-3.3.2-19.fc20

### 188642 - Fedora Linux 20 FEDORA-2014-16214 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1693

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16214

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146184.html>

Fedora Core 20

erlang-R16B-03.10.fc20

### 188644 - Fedora Linux 19 FEDORA-2014-15079 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1609, CVE-2014-7146, CVE-2014-8554, CVE-2014-8598

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15079

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145757.html>

Fedora Core 19

mantis-1.2.17-4.fc19

### 188646 - Fedora Linux 19 FEDORA-2014-16251 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

#### Description

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

FEDORA-2014-16251

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146152.html>

Fedora Core 19

mingw-flac-1.3.1-1.fc19

### **188650 - Fedora Linux 20 FEDORA-2014-15108 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-1609, CVE-2014-7146, CVE-2014-8554, CVE-2014-8598

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15108

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145944.html>

Fedora Core 20

mantis-1.2.17-4.fc20

### **188651 - Fedora Linux 21 FEDORA-2014-15142 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-1609, CVE-2014-7146, CVE-2014-8554, CVE-2014-8598

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15142

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145894.html>

Fedora Core 21

mantis-1.2.17-4.fc21

### **188656 - Fedora Linux 21 FEDORA-2014-16148 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8962, CVE-2014-9028

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16148

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146167.html>

Fedora Core 21

mingw-flac-1.3.1-1.fc21

### **188668 - Fedora Linux 21 FEDORA-2014-15951 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-0150, CVE-2014-8594, CVE-2014-8595, CVE-2014-9030

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15951

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145761.html>

Fedora Core 21

xen-4.4.1-9.fc21

### **17477 - (SOL15868) F5 BIG-IP Multiple Wireshark Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-4074, CVE-2013-4075, CVE-2013-4076, CVE-2013-4077, CVE-2013-4078, CVE-2013-4079, CVE-2013-4080, CVE-2013-4081, CVE-2013-4082, CVE-2013-4083, CVE-2013-4920, CVE-2013-4921, CVE-2013-4922, CVE-2013-4923, CVE-2013-4924, CVE-2013-4925, CVE-2013-4926, CVE-2013-4927, CVE-2013-4928, CVE-2013-4929, CVE-2013-4930, CVE-2013-4931, CVE-2013-4932, CVE-2013-4933, CVE-2013-4934, CVE-2013-4935, CVE-2013-4936

#### Description

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems.

#### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in several Wireshark dissectors and file parsers. Successful exploitation could allow an attacker to cause a denial of service condition.

### 17526 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 31.3

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

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

#### Observation

Mozilla Firefox ESR is an open source web browser.

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

### 17527 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 31.3

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

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

#### Observation

Mozilla Firefox ESR is an open source web browser.

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

### 17528 - Opera Multiple Vulnerabilities Prior To 26

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Description

Multiple unspecified vulnerabilities are present in some versions of Opera.

#### Observation

Opera is a popular web browser.

Multiple unspecified vulnerabilities are present in some versions of Opera. The flaws lie in the embedded Chromium engine. Successful exploitation could allow an attacker to cause unknown impact.

### 17535 - (HT6598) Apple iOS Multiple Vulnerabilities Prior To 8.1.2

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2014-4451, CVE-2014-4452, CVE-2014-4453, CVE-2014-4455, CVE-2014-4457, CVE-2014-4460, CVE-2014-4461, CVE-

2014-4462, CVE-2014-4463

### Description

Multiple vulnerabilities are present in some versions of Apple iOS.

### Observation

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

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose potentially sensitive information, bypass certain security restrictions, cause a denial of service, and execute arbitrary code.

## **85841 - CentOS 6, 7 CESA-2014-1983 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

### Description

The scan detected that the host is missing the following update:  
CESA-2014-1983

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020823.html>  
<http://lists.centos.org/pipermail/centos-announce/2014-December/020824.html>

#### CentOS 7

x86\_64

xorg-x11-server-Xnest-1.15.0-7.el7\_0.3  
xorg-x11-server-devel-1.15.0-7.el7\_0.3  
xorg-x11-server-common-1.15.0-7.el7\_0.3  
xorg-x11-server-Xvfb-1.15.0-7.el7\_0.3  
xorg-x11-server-Xdmx-1.15.0-7.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.el7\_0.3

i686

xorg-x11-server-devel-1.15.0-7.el7\_0.3

noarch

xorg-x11-server-source-1.15.0-7.el7\_0.3

#### CentOS 6

x86\_64

xorg-x11-server-Xdmx-1.15.0-25.el6.centos  
xorg-x11-server-common-1.15.0-25.el6.centos  
xorg-x11-server-Xephyr-1.15.0-25.el6.centos  
xorg-x11-server-Xorg-1.15.0-25.el6.centos  
xorg-x11-server-Xvfb-1.15.0-25.el6.centos  
xorg-x11-server-devel-1.15.0-25.el6.centos  
xorg-x11-server-Xnest-1.15.0-25.el6.centos

i686

xorg-x11-server-Xdmx-1.15.0-25.el6.centos  
xorg-x11-server-common-1.15.0-25.el6.centos  
xorg-x11-server-Xephyr-1.15.0-25.el6.centos  
xorg-x11-server-Xorg-1.15.0-25.el6.centos  
xorg-x11-server-Xvfb-1.15.0-25.el6.centos  
xorg-x11-server-devel-1.15.0-25.el6.centos  
xorg-x11-server-Xnest-1.15.0-25.el6.centos

noarch  
xorg-x11-server-source-1.15.0-25.el6.centos

### 85843 - CentOS 5 CESA-2014-1982 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

#### Description

The scan detected that the host is missing the following update:  
CESA-2014-1982

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020825.html>

CentOS 5

x86\_64

xorg-x11-server-sdk-1.1.1-48.107.el5.centos  
xorg-x11-server-Xvfb-1.1.1-48.107.el5.centos  
xorg-x11-server-Xorg-1.1.1-48.107.el5.centos  
xorg-x11-server-Xdmx-1.1.1-48.107.el5.centos  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5.centos  
xorg-x11-server-Xnest-1.1.1-48.107.el5.centos  
xorg-x11-server-Xephyr-1.1.1-48.107.el5.centos

i386

xorg-x11-server-sdk-1.1.1-48.107.el5.centos  
xorg-x11-server-Xvfb-1.1.1-48.107.el5.centos  
xorg-x11-server-Xorg-1.1.1-48.107.el5.centos  
xorg-x11-server-Xdmx-1.1.1-48.107.el5.centos  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5.centos  
xorg-x11-server-Xnest-1.1.1-48.107.el5.centos  
xorg-x11-server-Xephyr-1.1.1-48.107.el5.centos

### 88650 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-344-04 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

#### Description

The scan detected that the host is missing the following update:  
SSA:2014-344-04



### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.514137>

Slackware 13.0

x86\_64

openvpn-2.3.6-x86\_64-1

Slackware 14.1

x86\_64

openvpn-2.3.6-x86\_64-1

Slackware 13.37

x86\_64

openvpn-2.3.6-x86\_64-1

Slackware 13.1

x86\_64

openvpn-2.3.6-x86\_64-1

Slackware 14.0

x86\_64

openvpn-2.3.6-x86\_64-1

### **88651 - Slackware Linux 13.37, 14.0, 14.1 SSA:2014-344-07 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3686

### Description

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

SSA:2014-344-07

### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.441238>

Slackware 14.1

x86\_64

wpa\_supplicant-2.3-x86\_64-1

Slackware 13.37

x86\_64

wpa\_supplicant-0.7.3-x86\_64-4

Slackware 14.0

x86\_64

wpa\_supplicant-1.0-x86\_64-2

### **91684 - Oracle Enterprise Linux ELSA-2014-1982 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2013-6424, CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1982

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004721.html>

### OEL5

x86\_64

xorg-x11-server-Xdmx-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xvfb-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.0.1.el5\_11

### i386

xorg-x11-server-Xdmx-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xvfb-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.0.1.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.0.1.el5\_11

## 91685 - Oracle Enterprise Linux ELSA-2014-3103 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3182, CVE-2014-3186, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4656, CVE-2014-6410

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-3103

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004715.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004716.html>

### OEL6

x86\_64

kernel-uek-debug-3.8.13-55.1.1.el6uek  
kernel-uek-3.8.13-55.1.1.el6uek  
dtrace-modules-3.8.13-55.1.1.el6uek-0.4.3-4.el6  
kernel-uek-doc-3.8.13-55.1.1.el6uek

kernel-uek-devel-3.8.13-55.1.1.el6uek  
kernel-uek-firmware-3.8.13-55.1.1.el6uek  
kernel-uek-debug-devel-3.8.13-55.1.1.el6uek

OEL7

x86\_64  
kernel-uek-doc-3.8.13-55.1.1.el7uek  
dtrace-modules-3.8.13-55.1.1.el7uek-0.4.3-4.el7  
kernel-uek-debug-devel-3.8.13-55.1.1.el7uek  
kernel-uek-3.8.13-55.1.1.el7uek  
kernel-uek-firmware-3.8.13-55.1.1.el7uek  
kernel-uek-devel-3.8.13-55.1.1.el7uek  
kernel-uek-debug-3.8.13-55.1.1.el7uek

## 91691 - Oracle Enterprise Linux ELSA-2014-1983 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1983

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004713.html>  
<http://oss.oracle.com/pipermail/el-errata/2014-December/004714.html>

OEL6

x86\_64  
xorg-x11-server-Xvfb-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-devel-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6  
xorg-x11-server-Xdmx-1.15.0-25.el6\_6  
xorg-x11-server-source-1.15.0-25.el6\_6  
xorg-x11-server-Xnest-1.15.0-25.el6\_6  
xorg-x11-server-Xorg-1.15.0-25.el6\_6

i386

xorg-x11-server-Xvfb-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-devel-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6  
xorg-x11-server-Xdmx-1.15.0-25.el6\_6  
xorg-x11-server-source-1.15.0-25.el6\_6  
xorg-x11-server-Xnest-1.15.0-25.el6\_6  
xorg-x11-server-Xorg-1.15.0-25.el6\_6

OEL7

x86\_64  
xorg-x11-server-Xnest-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-common-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.0.1.el7\_0.3

xorg-x11-server-source-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-devel-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-Xvfb-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-Xdmx-1.15.0-7.0.1.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.0.1.el7\_0.3

## 91692 - Oracle Enterprise Linux ELSA-2014-3104 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-1739, CVE-2014-3181, CVE-2014-3186, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4656, CVE-2014-6410

### Description

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

ELSA-2014-3104

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2014-December/004719.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004717.html>

### OEL6

x86\_64

kernel-uek-debug-devel-2.6.39-400.215.14.el6uek

kernel-uek-2.6.39-400.215.14.el6uek

kernel-uek-debug-2.6.39-400.215.14.el6uek

kernel-uek-doc-2.6.39-400.215.14.el6uek

kernel-uek-firmware-2.6.39-400.215.14.el6uek

kernel-uek-devel-2.6.39-400.215.14.el6uek

i386

kernel-uek-debug-devel-2.6.39-400.215.14.el6uek

kernel-uek-2.6.39-400.215.14.el6uek

kernel-uek-devel-2.6.39-400.215.14.el6uek

kernel-uek-firmware-2.6.39-400.215.14.el6uek

kernel-uek-debug-2.6.39-400.215.14.el6uek

kernel-uek-doc-2.6.39-400.215.14.el6uek

### OEL5

x86\_64

kernel-uek-debug-2.6.39-400.215.14.el5uek

kernel-uek-firmware-2.6.39-400.215.14.el5uek

kernel-uek-devel-2.6.39-400.215.14.el5uek

kernel-uek-debug-devel-2.6.39-400.215.14.el5uek

kernel-uek-2.6.39-400.215.14.el5uek

kernel-uek-doc-2.6.39-400.215.14.el5uek

i386

kernel-uek-firmware-2.6.39-400.215.14.el5uek

kernel-uek-doc-2.6.39-400.215.14.el5uek

kernel-uek-2.6.39-400.215.14.el5uek

kernel-uek-debug-2.6.39-400.215.14.el5uek

kernel-uek-debug-devel-2.6.39-400.215.14.el5uek

kernel-uek-devel-2.6.39-400.215.14.el5uek

## 93440 - Mandriva Linux MBS1 MDVSA-2014-246 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-246

### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A246/>

Mandriva Linux mbs1  
x86\_64  
openvpn-2.3.2-1  
lib64openvpn-devel-2.3.2-1

## 130024 - Debian Linux 7.0 DSA-3095-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

### Description

The scan detected that the host is missing the following update:  
DSA-3095-1

### Observation

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

<http://www.debian.org/security/2014/dsa-3095>

Debian 7.0  
all  
xnest\_1.12.4-6+deb7u5  
xserver-xorg-core-udeb\_1.12.4-6+deb7u5  
xdmx-tools\_1.12.4-6+deb7u5  
xserver-xorg-dev\_1.12.4-6+deb7u5  
xvfb\_1.12.4-6+deb7u5  
xserver-common\_1.12.4-6+deb7u5  
xserver-xephyr\_1.12.4-6+deb7u5  
xserver-xorg-core-dbg\_1.12.4-6+deb7u5  
xserver-xorg-core\_1.12.4-6+deb7u5  
xdmx\_1.12.4-6+deb7u5  
xserver-xfbdev\_1.12.4-6+deb7u5

## 139040 - Oracle Solaris 11.2.5.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: Medium

CVE: CVE-2014-0012, CVE-2014-1402, CVE-2014-2285, CVE-2014-3248, CVE-2014-3250, CVE-2014-3565, CVE-2014-3707, CVE-2014-4341, CVE-2014-4342

#### Description

The scan detected that the host is missing the following update:  
SRU 11.2.5.5.0

#### Observation

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

<https://support.oracle.com/rs?type=doc&id=1914034.1>

<http://www.oracle.com/technetwork/topics/security/thirdparty-patch-map-1482893.html>

### **140638 - Red Hat Enterprise Linux RHSA-2014-1982 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

#### Description

The scan detected that the host is missing the following update:  
RHSA-2014-1982

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1982.html>

#### RHEL5D

x86\_64

xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

i386

xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

#### RHEL5S

x86\_64

xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.el5\_11

xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

i386

xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

## 140642 - Red Hat Enterprise Linux RHSA-2014-1983 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

### Description

The scan detected that the host is missing the following update:  
RHSA-2014-1983

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1983.html>

### RHEL7WS

x86\_64  
xorg-x11-server-common-1.15.0-7.el7\_0.3  
xorg-x11-server-debuginfo-1.15.0-7.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.el7\_0.3

### RHEL7D

x86\_64  
xorg-x11-server-common-1.15.0-7.el7\_0.3  
xorg-x11-server-debuginfo-1.15.0-7.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.el7\_0.3

### RHEL6D

x86\_64  
xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

i386

xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

## RHEL6S

x86\_64

xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

i386

xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

## RHEL7S

x86\_64

xorg-x11-server-common-1.15.0-7.el7\_0.3  
xorg-x11-server-debuginfo-1.15.0-7.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.el7\_0.3

## RHEL6WS

x86\_64

xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

i386

xorg-x11-server-Xorg-1.15.0-25.el6\_6  
xorg-x11-server-common-1.15.0-25.el6\_6  
xorg-x11-server-debuginfo-1.15.0-25.el6\_6  
xorg-x11-server-Xephyr-1.15.0-25.el6\_6

### 142562 - SuSE SLES 11 SP2 firefox-201412-10065 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

The scan detected that the host is missing the following update:  
firefox-201412-10065

#### Observation

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

<https://download.suse.com/Download?buildid=hZDH3ewXVg0~>  
<https://download.suse.com/Download?buildid=Fna6R8VE6Vs~>  
<https://download.suse.com/Download?buildid=5ymvcjTcQ5Q~>

SuSE SLES 11 SP2

x86\_64

MozillaFirefox-translations-31.3.0esr-0.3.1  
MozillaFirefox-31.3.0esr-0.3.1

i586



MozillaFirefox-translations-31.3.0esr-0.3.1  
MozillaFirefox-31.3.0esr-0.3.1

### 142564 - SuSE Linux 12.3 openSUSE-SU-2014:1647-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2011-3368, CVE-2012-2687, CVE-2013-1862, CVE-2013-1896, CVE-2013-6438, CVE-2014-0098, CVE-2014-0226, CVE-2014-0231

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1647-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00065.html>

SuSE Linux 12.3

i586

apache2-2.2.29-10.16.1

apache2-doc-2.2.29-10.16.1

apache2-debugsource-2.2.29-10.16.1

apache2-debuginfo-2.2.29-10.16.1

apache2-prefork-2.2.29-10.16.1

apache2-itk-debuginfo-2.2.29-10.16.1

apache2-worker-2.2.29-10.16.1

apache2-devel-2.2.29-10.16.1

apache2-utils-2.2.29-10.16.1

apache2-worker-debuginfo-2.2.29-10.16.1

apache2-prefork-debuginfo-2.2.29-10.16.1

apache2-itk-2.2.29-10.16.1

apache2-example-pages-2.2.29-10.16.1

apache2-event-2.2.29-10.16.1

apache2-utils-debuginfo-2.2.29-10.16.1

apache2-event-debuginfo-2.2.29-10.16.1

### 142568 - SuSE SLES 11 SP3, SLED 11 SP3 firefox-201412-10064 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

The scan detected that the host is missing the following update:  
firefox-201412-10064

#### Observation

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

<https://download.suse.com/Download?buildid=ubrsrayGSu9M~>

[https://download.suse.com/Download?buildid=\\_mkswRPCuiM~](https://download.suse.com/Download?buildid=_mkswRPCuiM~)

<https://download.suse.com/Download?buildid=ScRUEwMPqr4~>  
<https://download.suse.com/Download?buildid=e1tAR0d0oh8~>  
<https://download.suse.com/Download?buildid=YGjrxEU7GDY~>  
<https://download.suse.com/Download?buildid=qavZ2X-NzyA~>  
<https://download.suse.com/Download?buildid=3mmAkTv2ObQ~>  
<https://download.suse.com/Download?buildid=-hOCKhOFtI0~>  
[https://download.suse.com/Download?buildid=osF\\_Zt1Wjxc~](https://download.suse.com/Download?buildid=osF_Zt1Wjxc~)

SuSE SLED 11 SP3

x86\_64

MozillaFirefox-31.3.0esr-0.8.1

MozillaFirefox-translations-31.3.0esr-0.8.1

i586

MozillaFirefox-31.3.0esr-0.8.1

MozillaFirefox-translations-31.3.0esr-0.8.1

SuSE SLES 11 SP3

x86\_64

MozillaFirefox-31.3.0esr-0.8.1

MozillaFirefox-translations-31.3.0esr-0.8.1

i586

MozillaFirefox-31.3.0esr-0.8.1

MozillaFirefox-translations-31.3.0esr-0.8.1

#### 142575 - SuSE SLES 10 SP4 firefox-201412-9009 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

#### Description

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

firefox-201412-9009

#### Observation

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

For more information see:

<https://download.suse.com/Download?buildid=G0U6fdqQdvw~>  
[https://download.suse.com/Download?buildid=ExjHNg\\_OVys~](https://download.suse.com/Download?buildid=ExjHNg_OVys~)  
<https://download.suse.com/Download?buildid=aWDeQM06vxE~>  
[https://download.suse.com/Download?buildid=gS\\_uwxUv9tM~](https://download.suse.com/Download?buildid=gS_uwxUv9tM~)  
<https://download.suse.com/Download?buildid=AjaMYNvJhh4~>  
<https://download.suse.com/Download?buildid=9pdyETmFLIE~>

SuSE SLES 10 SP4

i586

MozillaFirefox-translations-31.3.0esr-0.5.1

MozillaFirefox-31.3.0esr-0.5.1

MozillaFirefox-debuginfo-31.3.0esr-0.5.1

#### 170436 - Amazon Linux AMI ALAS-2014-459 Update Is Not Installed

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

Risk Level: Medium  
CVE: CVE-2014-8104

#### Description

The scan detected that the host is missing the following update:  
ALAS-2014-459

#### Observation

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

<https://alas.aws.amazon.com/ALAS-2014-459.html>

Amazon Linux AMI  
x86\_64  
openvpn-debuginfo-2.3.6-1.12.amzn1  
openvpn-2.3.6-1.12.amzn1

i686  
openvpn-debuginfo-2.3.6-1.12.amzn1  
openvpn-2.3.6-1.12.amzn1

### **174605 - Scientific Linux Security ERRATA Important: xorg-x11-server on SL6.x, SL7.x i386/x86\_64 (1412-1959)**

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102, CVE-2014-8103

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: xorg-x11-server on SL6.x, SL7.x i386/x86\_64 (1412-1959)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1959>

SL7  
x86\_64  
xorg-x11-server-debuginfo-1.15.0-7.el7\_0.3  
xorg-x11-server-Xnest-1.15.0-7.el7\_0.3  
xorg-x11-server-Xdmx-1.15.0-7.el7\_0.3  
xorg-x11-server-devel-1.15.0-7.el7\_0.3  
xorg-x11-server-Xvfb-1.15.0-7.el7\_0.3  
xorg-x11-server-Xorg-1.15.0-7.el7\_0.3  
xorg-x11-server-common-1.15.0-7.el7\_0.3  
xorg-x11-server-Xephyr-1.15.0-7.el7\_0.3

noarch  
xorg-x11-server-source-1.15.0-7.el7\_0.3

SL6  
x86\_64  
xorg-x11-server-Xorg-1.15.0-25.sl6  
xorg-x11-server-devel-1.15.0-25.sl6

xorg-x11-server-debuginfo-1.15.0-25.sl6  
xorg-x11-server-Xnest-1.15.0-25.sl6  
xorg-x11-server-common-1.15.0-25.sl6  
xorg-x11-server-Xvfb-1.15.0-25.sl6  
xorg-x11-server-Xephyr-1.15.0-25.sl6  
xorg-x11-server-Xdmx-1.15.0-25.sl6

i386

xorg-x11-server-Xorg-1.15.0-25.sl6  
xorg-x11-server-devel-1.15.0-25.sl6  
xorg-x11-server-debuginfo-1.15.0-25.sl6  
xorg-x11-server-Xnest-1.15.0-25.sl6  
xorg-x11-server-common-1.15.0-25.sl6  
xorg-x11-server-Xvfb-1.15.0-25.sl6  
xorg-x11-server-Xephyr-1.15.0-25.sl6  
xorg-x11-server-Xdmx-1.15.0-25.sl6

noarch

xorg-x11-server-source-1.15.0-25.sl6

### 174608 - Scientific Linux Security ERRATA Important: xorg-x11-server on SL5.x i386/x86\_64 (1412-1823)

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

#### Description

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

Security ERRATA Important: xorg-x11-server on SL5.x i386/x86\_64 (1412-1823)

#### Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=1823>

SL5

x86\_64

xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

i386

xorg-x11-server-debuginfo-1.1.1-48.107.el5\_11  
xorg-x11-server-Xephyr-1.1.1-48.107.el5\_11  
xorg-x11-server-Xnest-1.1.1-48.107.el5\_11  
xorg-x11-server-sdk-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvfb-1.1.1-48.107.el5\_11  
xorg-x11-server-Xvnc-source-1.1.1-48.107.el5\_11  
xorg-x11-server-Xdmx-1.1.1-48.107.el5\_11  
xorg-x11-server-Xorg-1.1.1-48.107.el5\_11

## 178009 - Gentoo Linux GLSA-201412-14 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-4227, CVE-2009-4228

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-14

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-14.xml>

Affected packages:

media-gfx/xfig < 3.2.5c

## 178013 - Gentoo Linux GLSA-201412-22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0480, CVE-2014-0481, CVE-2014-0482, CVE-2014-0483

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-22

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-22.xml>

Affected packages:

dev-python/django < 1.6.7

## 178014 - Gentoo Linux GLSA-201412-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3477, CVE-2014-3532, CVE-2014-3533, CVE-2014-3635, CVE-2014-3636, CVE-2014-3637, CVE-2014-3638, CVE-2014-3639, CVE-2014-7824

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-12

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-12.xml>

Affected packages:  
sys-apps/dbus < 1.8.10

### 178018 - Gentoo Linux GLSA-201412-26 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-2338, CVE-2014-2891

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-26

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-26.xml>

Affected packages:

net-misc/strongswan < 5.1.3

### 178023 - Gentoo Linux GLSA-201412-15 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3248, CVE-2014-3251

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-15

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-15.xml>

Affected packages:

app-admin/mcollective < 2.5.3

### 178024 - Gentoo Linux GLSA-201412-29 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2733, CVE-2012-3544, CVE-2012-3546, CVE-2012-4431, CVE-2012-4534, CVE-2012-5885, CVE-2012-5886, CVE-2012-5887, CVE-2013-2067, CVE-2013-2071, CVE-2013-4286, CVE-2013-4322, CVE-2013-4590, CVE-2014-0033, CVE-2014-0050, CVE-2014-0075, CVE-2014-0096, CVE-2014-0099, CVE-2014-0119

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-29

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-29.xml>

Affected packages:  
www-servers/tomcat < 7.0.56

### **178026 - Gentoo Linux GLSA-201412-21 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-0240, CVE-2014-0242

### Description

The scan detected that the host is missing the following update:  
GLSA-201412-21

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-21.xml>

Affected packages:  
www-apache/mod\_wsgi < 3.5

### **181301 - FreeBSD xserver Multiple Issue With X Client Request Handling (27b9b2f0-8081-11e4-b4ca-bcaec565249c)**

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

Risk Level: Medium

CVE: CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102

### Description

The scan detected that the host is missing the following update:  
xserver -- multiple issue with X client request handling (27b9b2f0-8081-11e4-b4ca-bcaec565249c)

### Observation

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

<http://www.vuxml.org/freebsd/27b9b2f0-8081-11e4-b4ca-bcaec565249c.html>

Affected packages:  
xorg-server < 1.12.4\_10,1

### **184646 - Ubuntu Linux 12.04 USN-2444-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-7825, CVE-2014-7826, CVE-2014-7841, CVE-2014-8134, CVE-2014-8884, CVE-2014-9090

### Description

The scan detected that the host is missing the following update:  
USN-2444-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002765.html>

Ubuntu 12.04

linux-image-3.2.0-1457-omap4\_3.2.0-1457.77

## **184651 - Ubuntu Linux 12.04 USN-2443-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-7825, CVE-2014-7826, CVE-2014-7841, CVE-2014-8134, CVE-2014-8884, CVE-2014-9090

### Description

The scan detected that the host is missing the following update:  
USN-2443-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002764.html>

Ubuntu 12.04

linux-image-3.2.0-74-omap\_3.2.0-74.109

linux-image-3.2.0-74-virtual\_3.2.0-74.109

linux-image-3.2.0-74-generic-pae\_3.2.0-74.109

linux-image-3.2.0-74-powerpc-smp\_3.2.0-74.109

linux-image-3.2.0-74-generic\_3.2.0-74.109

linux-image-3.2.0-74-powerpc64-smp\_3.2.0-74.109

linux-image-3.2.0-74-highbank\_3.2.0-74.109

## **188613 - Fedora Linux 20 FEDORA-2014-16243 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3635, CVE-2014-3636, CVE-2014-3637, CVE-2014-3638, CVE-2014-3639, CVE-2014-7824

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16243

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146098.html>



Fedora Core 20

dbus-1.6.28-1.fc20

### 188619 - Fedora Linux 20 FEDORA-2014-16273 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16273

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146073.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146072.html>

Fedora Core 20

pkcs11-helper-1.11-3.fc20

openvpn-2.3.6-1.fc20

### 188637 - Fedora Linux 21 FEDORA-2014-16060 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16060

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145833.html>

Fedora Core 21

openvpn-2.3.6-1.fc21

### 188673 - Fedora Linux 19 FEDORA-2014-16234 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8104

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16234

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146029.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146030.html>

Fedora Core 19

pkcs11-helper-1.11-3.fc19  
openvpn-2.3.6-1.fc19

## **17425 - (HPSBUX03188) HP-UX HP Secure Shell Multiple Vulnerabilities**

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

Risk Level: Medium

CVE: CVE-2013-4548, CVE-2014-1692, CVE-2014-2532, CVE-2014-2653

### Description

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

### Observation

HP-UX is an operating system developed by HP.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in secure shell component. Successful exploitation could allow an attacker to bypass security restrict or cause denial of service.

## **17449 - WordPress Bulletproof Security Plugin "dbhost" Cross-Site Scripting Vulnerability**

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

Risk Level: Medium

CVE: CVE-2014-7958

### Description

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

### Observation

WordPress is a popular blog web application.

A Cross-site scripting vulnerability is present in some versions of Bulletproof Security Plugin for WordPress. The flaw lies in the bpsunlock.php component which does not properly sanitize the dbhost parameter. Successful exploitation could allow an attacker to execute remote code.

## **17469 - (SOL15881) F5 BIG-IP Libpng Heap Buffer Overflow Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2011-3048

### Description

A denial of service vulnerability is present in some versions of F5 BIG-IP systems.

#### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the png\_set\_text\_2 function in pngset.c in libpng. Successful exploitation could allow an attacker to cause a denial of service condition.

### **17479 - Cisco Adaptive Security Appliance (ASA) SSL VPN Denial of Service Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3407

#### Description

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

#### Observation

Cisco Adaptive Security Appliances (ASA) is a security and firewall device.

A vulnerability in some versions of Cisco Adaptive Security Appliance could lead to a denial of service. The flaw is due to improper input validation in the WebVPN portal. Successful exploitation by a remote attacker could result in a denial of service condition.

### **17480 - (SOL15885) F5 BIG-IP GNU C Library Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2011-1071

#### Description

A denial of service vulnerability is present in some versions of F5 BIG-IP systems.

#### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the GNU C library. Successful exploitation could allow an attacker to cause a denial of service condition.

### **17496 - (SOL15605) F5 BIG-IP XML Entity Injection Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-6032, CVE-2014-6033

#### Description

Multiple XML external entity (XXE) vulnerabilities are present in some versions of F5 BIG-IP systems.

#### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

Multiple XML external entity (XXE) vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws are identified in the BIG-IP Configuration utility and the Enterprise Manager Configuration utility. Successful exploitation could allow a remote authenticated attacker to retrieve arbitrary files and cause a denial of service.

## 17516 - (HT6596) Apple Safari Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2014-1748, CVE-2014-4452, CVE-2014-4459, CVE-2014-4465, CVE-2014-4466, CVE-2014-4468, CVE-2014-4469, CVE-2014-4470, CVE-2014-4471, CVE-2014-4472, CVE-2014-4473, CVE-2014-4474, CVE-2014-4475

### 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 and Safari core components. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

## 17531 - (VMSA-2014-0012) VMware ESXi Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2013-2877, CVE-2013-4238, CVE-2014-0015, CVE-2014-0138, CVE-2014-0191

### Description

Multiple vulnerabilities are present in some versions of VMware ESXi.

### Observation

VMware ESXi is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware ESXi. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or to authenticate as other users.

## 17532 - (VMSA-2014-0012) VMware ESXi Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-1752, CVE-2013-2877, CVE-2013-4238, CVE-2014-0015, CVE-2014-0138, CVE-2014-0191

### Description

Multiple vulnerabilities are present in some versions of VMware ESXi.

### Observation

VMware ESXi is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware ESXi. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service condition or to authenticate as other users.

## 17533 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.3

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

### Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

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

## **17534 - Mozilla Thunderbird Multiple Vulnerabilities Prior To 31.3**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

### Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

### Observation

Mozilla Thunderbird is an open-source Email, newsgroup, news feed, and chat client.

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

## **17540 - (SOL15876) F5 BIG-IP PHP Heap Buffer Overflow Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-2110

### Description

A buffer overflow vulnerability is present in some versions of F5 BIG-IP systems.

### Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A buffer overflow vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the PHP component. Successful exploitation could allow an attacker to cause a denial of service.

## **17545 - (APSB14-29) Adobe ColdFusion Resource Consumption Denial of Service**

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

Risk Level: Medium

CVE: CVE-2014-9166

### Description

A denial of service vulnerability is present in some versions of Adobe ColdFusion.

### Observation

Adobe ColdFusion is a web application development platform.

A denial of service vulnerability is present in some versions of Adobe ColdFusion. The flaw is caused due to a resource consumption defect. Successful exploitation by a remote attacker could result in a denial of service condition.

### 85842 - CentOS 6, 7 CESA-2014-1999 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-2771, CVE-2014-7844

#### Description

The scan detected that the host is missing the following update:  
CESA-2014-1999

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2014-December/020837.html>

<http://lists.centos.org/pipermail/centos-announce/2014-December/020836.html>

CentOS 7  
x86\_64  
mailx-12.5-12.el7\_0

CentOS 6  
x86\_64  
mailx-12.4-8.el6\_6

i686  
mailx-12.4-8.el6\_6

### 91689 - Oracle Enterprise Linux ELSA-2014-3105 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3184, CVE-2014-3688, CVE-2014-4652, CVE-2014-4656, CVE-2014-6410

#### Description

The scan detected that the host is missing the following update:  
ELSA-2014-3105

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004718.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004720.html>

OEL6  
x86\_64  
kernel-uek-doc-2.6.32-400.36.12.el6uek  
ofa-2.6.32-400.36.12.el6uek-1.5.1-4.0.58  
ofa-2.6.32-400.36.12.el6uekdebug-1.5.1-4.0.58  
kernel-uek-headers-2.6.32-400.36.12.el6uek  
kernel-uek-devel-2.6.32-400.36.12.el6uek

mlnx\_en-2.6.32-400.36.12.el6uekdebug-1.5.7-0.1  
kernel-uek-firmware-2.6.32-400.36.12.el6uek  
kernel-uek-2.6.32-400.36.12.el6uek  
kernel-uek-debug-2.6.32-400.36.12.el6uek  
kernel-uek-debug-devel-2.6.32-400.36.12.el6uek  
mlnx\_en-2.6.32-400.36.12.el6uek-1.5.7-0.1

i386

kernel-uek-doc-2.6.32-400.36.12.el6uek  
ofa-2.6.32-400.36.12.el6uek-1.5.1-4.0.58  
ofa-2.6.32-400.36.12.el6uekdebug-1.5.1-4.0.58  
kernel-uek-headers-2.6.32-400.36.12.el6uek  
kernel-uek-devel-2.6.32-400.36.12.el6uek  
mlnx\_en-2.6.32-400.36.12.el6uekdebug-1.5.7-0.1  
kernel-uek-firmware-2.6.32-400.36.12.el6uek  
kernel-uek-2.6.32-400.36.12.el6uek  
kernel-uek-debug-2.6.32-400.36.12.el6uek  
kernel-uek-debug-devel-2.6.32-400.36.12.el6uek  
mlnx\_en-2.6.32-400.36.12.el6uek-1.5.7-0.1

OEL5

x86\_64

kernel-uek-doc-2.6.32-400.36.12.el5uek  
kernel-uek-firmware-2.6.32-400.36.12.el5uek  
ofa-2.6.32-400.36.12.el5uek-1.5.1-4.0.58  
kernel-uek-headers-2.6.32-400.36.12.el5uek  
kernel-uek-devel-2.6.32-400.36.12.el5uek  
kernel-uek-debug-devel-2.6.32-400.36.12.el5uek  
kernel-uek-2.6.32-400.36.12.el5uek  
kernel-uek-debug-2.6.32-400.36.12.el5uek  
mlnx\_en-2.6.32-400.36.12.el5uekdebug-1.5.7-2  
mlnx\_en-2.6.32-400.36.12.el5uek-1.5.7-2  
ofa-2.6.32-400.36.12.el5uekdebug-1.5.1-4.0.58

i386

kernel-uek-doc-2.6.32-400.36.12.el5uek  
kernel-uek-firmware-2.6.32-400.36.12.el5uek  
ofa-2.6.32-400.36.12.el5uek-1.5.1-4.0.58  
kernel-uek-headers-2.6.32-400.36.12.el5uek  
kernel-uek-devel-2.6.32-400.36.12.el5uek  
kernel-uek-debug-devel-2.6.32-400.36.12.el5uek  
kernel-uek-2.6.32-400.36.12.el5uek  
kernel-uek-debug-2.6.32-400.36.12.el5uek  
mlnx\_en-2.6.32-400.36.12.el5uekdebug-1.5.7-2  
mlnx\_en-2.6.32-400.36.12.el5uek-1.5.7-2  
ofa-2.6.32-400.36.12.el5uekdebug-1.5.1-4.0.58

## 91693 - Oracle Enterprise Linux ELSA-2014-1999 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-2771, CVE-2014-7844

### Description

The scan detected that the host is missing the following update:  
ELSA-2014-1999

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2014-December/004736.html>

<http://oss.oracle.com/pipermail/el-errata/2014-December/004735.html>

OEL6

x86\_64

mailx-12.4-8.el6\_6

i386

mailx-12.4-8.el6\_6

OEL7

x86\_64

mailx-12.5-12.el7\_0

### 93434 - Mandriva Linux MBS1 MDVSA-2014-245 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9116

#### Description

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

MDVSA-2014-245

#### Observation

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

For more information see:

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A245/>

Mandriva Linux mbs1

x86\_64

mutt-utf8-1.5.23-1

mutt-1.5.23-1

mutt-doc-1.5.23-1

### 93441 - Mandriva Linux MBS1 MDVSA-2014-242 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

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

MDVSA-2014-242

#### Observation

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

For more information see:

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A242/>

Mandriva Linux mbs1



x86\_64  
lib64yaml0\_2-0.1.6-1.1  
perl-yaml-libyaml-0.380.0-2.3  
lib64yaml-devel-0.1.6-1.1

### 130019 - Debian Linux 7.0 DSA-3103-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

The scan detected that the host is missing the following update:  
DSA-3103-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3103>

Debian 7.0  
all  
libyaml-libyaml-perl\_0.38-3+deb7u3

### 130022 - Debian Linux 7.0 DSA-3096-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8601

#### Description

The scan detected that the host is missing the following update:  
DSA-3096-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3096>

Debian 7.0  
all  
pdns-recursor\_3.3-3+deb7u1

### 130026 - Debian Linux 7.0 DSA-3102-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

The scan detected that the host is missing the following update:  
DSA-3102-1

## Observation

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

<http://www.debian.org/security/2014/dsa-3102>

Debian 7.0

all

libyaml-0-2\_0.1.4-2+deb7u5

libyaml-0-2-dbg\_0.1.4-2+deb7u5

libyaml-dev\_0.1.4-2+deb7u5

## **140640 - Red Hat Enterprise Linux RHSA-2014-1999 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2004-2771, CVE-2014-7844

## Description

The scan detected that the host is missing the following update:  
RHSA-2014-1999

## Observation

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

<https://rhn.redhat.com/errata/RHSA-2014-1999.html>

RHEL7WS

x86\_64

mailx-debuginfo-12.5-12.el7\_0

mailx-12.5-12.el7\_0

RHEL7D

x86\_64

mailx-debuginfo-12.5-12.el7\_0

mailx-12.5-12.el7\_0

RHEL6D

x86\_64

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

i386

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

RHEL6S

x86\_64

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

i386

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

RHEL7S

x86\_64  
mailx-debuginfo-12.5-12.el7\_0  
mailx-12.5-12.el7\_0

RHEL6WS  
x86\_64  
mailx-debuginfo-12.4-8.el6\_6  
mailx-12.4-8.el6\_6

i386  
mailx-debuginfo-12.4-8.el6\_6  
mailx-12.4-8.el6\_6

### 142559 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1635-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9116

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1635-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00053.html>

SuSE Linux 13.1  
i586  
mutt-debuginfo-1.5.21-41.8.1  
mutt-1.5.21-41.8.1  
mutt-debugsource-1.5.21-41.8.1

SuSE Linux 12.3  
i586  
mutt-1.5.21-36.20.1  
mutt-debugsource-1.5.21-36.20.1  
mutt-debuginfo-1.5.21-36.20.1

SuSE Linux 13.2  
i586  
mutt-1.5.21-44.4.1  
mutt-debugsource-1.5.21-44.4.1  
mutt-debuginfo-1.5.21-44.4.1

### 142566 - SuSE SLED 11 SP3 finch-10078 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3695, CVE-2014-3696, CVE-2014-3698

#### Description

The scan detected that the host is missing the following update:  
finch-10078

## Observation

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

<https://download.suse.com/Download?buildid=ldfbgHvb3OA~>  
<https://download.suse.com/Download?buildid=06KQFcDB1hk~>

SuSE SLED 11 SP3

x86\_64

libpurple-lang-2.6.6-0.25.2

pidgin-2.6.6-0.25.2

finch-2.6.6-0.25.2

libpurple-meanwhile-2.6.6-0.25.2

libpurple-2.6.6-0.25.2

libpurple-tcl-2.6.6-0.25.2

i586

libpurple-lang-2.6.6-0.25.2

pidgin-2.6.6-0.25.2

finch-2.6.6-0.25.2

libpurple-meanwhile-2.6.6-0.25.2

libpurple-2.6.6-0.25.2

libpurple-tcl-2.6.6-0.25.2

## **142567 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1625-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-9130

## Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1625-1

## Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00047.html>

SuSE Linux 13.1

i586

libyaml-debugsource-0.1.4-2.16.1

libyaml-devel-0.1.4-2.16.1

libyaml-0-2-debuginfo-0.1.4-2.16.1

libyaml-0-2-0.1.4-2.16.1

SuSE Linux 12.3

i586

libyaml-devel-0.1.3-11.16.1

libyaml-0-2-0.1.3-11.16.1

libyaml-0-2-debuginfo-0.1.3-11.16.1

libyaml-debugsource-0.1.3-11.16.1

SuSE Linux 13.2

i586

libyaml-debugsource-0.1.6-2.4.1

libyaml-0-2-debuginfo-0.1.6-2.4.1  
libyaml-0-2-0.1.6-2.4.1  
libyaml-devel-0.1.6-2.4.1

### 142572 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1643-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9112

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1643-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00061.html>

SuSE Linux 13.1  
i586  
cpio-lang-2.11-25.4.1  
cpio-debugsource-2.11-25.4.1  
cpio-2.11-25.4.1  
cpio-debuginfo-2.11-25.4.1

SuSE Linux 12.3  
i586  
cpio-2.11-21.4.1  
cpio-debuginfo-2.11-21.4.1  
cpio-lang-2.11-21.4.1  
cpio-debugsource-2.11-21.4.1

SuSE Linux 13.2  
i586  
cpio-debuginfo-2.11-29.5.1  
cpio-2.11-29.5.1  
cpio-debugsource-2.11-29.5.1  
cpio-lang-2.11-29.5.1

### 142574 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1642-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1642-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00060.html>

SuSE Linux 13.1

x86\_64

firebird-doc-2.5.2.26539-8.4.1  
firebird-debuginfo-32bit-2.5.2.26539-8.4.1  
firebird-32bit-2.5.2.26539-8.4.1  
libfbclient2-debuginfo-32bit-2.5.2.26539-8.4.1  
libfbclient2-32bit-2.5.2.26539-8.4.1

i586

libfbembed2\_5-2.5.2.26539-8.4.1  
firebird-classic-debugsource-2.5.2.26539-8.4.1  
libfbembed2\_5-debuginfo-2.5.2.26539-8.4.1  
firebird-devel-2.5.2.26539-8.4.1  
firebird-classic-debuginfo-2.5.2.26539-8.4.1  
firebird-superserver-2.5.2.26539-8.4.1  
libfbclient2-2.5.2.26539-8.4.1  
firebird-debuginfo-2.5.2.26539-8.4.1  
libfbclient2-debuginfo-2.5.2.26539-8.4.1  
libfbembed-devel-2.5.2.26539-8.4.1  
libfbclient2-devel-2.5.2.26539-8.4.1  
firebird-classic-2.5.2.26539-8.4.1  
firebird-2.5.2.26539-8.4.1  
firebird-debugsource-2.5.2.26539-8.4.1  
firebird-superserver-debuginfo-2.5.2.26539-8.4.1

SuSE Linux 12.3

x86\_64

firebird-debuginfo-32bit-2.5.2.26539-2.9.1  
libfbclient2-32bit-2.5.2.26539-2.9.1  
libfbclient2-debuginfo-32bit-2.5.2.26539-2.9.1  
firebird-doc-2.5.2.26539-2.9.1  
firebird-32bit-2.5.2.26539-2.9.1

i586

firebird-superserver-debuginfo-2.5.2.26539-2.9.1  
libfbclient2-debuginfo-2.5.2.26539-2.9.1  
libfbembed-devel-2.5.2.26539-2.9.1  
firebird-classic-2.5.2.26539-2.9.1  
firebird-2.5.2.26539-2.9.1  
libfbembed2\_5-2.5.2.26539-2.9.1  
firebird-debugsource-2.5.2.26539-2.9.1  
firebird-superserver-2.5.2.26539-2.9.1  
libfbclient2-2.5.2.26539-2.9.1  
firebird-debuginfo-2.5.2.26539-2.9.1  
firebird-devel-2.5.2.26539-2.9.1  
libfbclient2-devel-2.5.2.26539-2.9.1  
firebird-classic-debugsource-2.5.2.26539-2.9.1  
firebird-classic-debuginfo-2.5.2.26539-2.9.1  
libfbembed2\_5-debuginfo-2.5.2.26539-2.9.1

SuSE Linux 13.2

x86\_64

firebird-debuginfo-32bit-2.5.2.26539-14.4.1  
libfbclient2-32bit-2.5.2.26539-14.4.1  
firebird-32bit-2.5.2.26539-14.4.1  
firebird-doc-2.5.2.26539-14.4.1  
libfbclient2-debuginfo-32bit-2.5.2.26539-14.4.1

i586

firebird-classic-debuginfo-2.5.2.26539-14.4.1

libfbembed2\_5-debuginfo-2.5.2.26539-14.4.1  
firebird-superserver-2.5.2.26539-14.4.1  
firebird-superserver-debuginfo-2.5.2.26539-14.4.1  
firebird-debuginfo-2.5.2.26539-14.4.1  
firebird-classic-2.5.2.26539-14.4.1  
firebird-classic-debugsource-2.5.2.26539-14.4.1  
firebird-devel-2.5.2.26539-14.4.1  
libfbembed-devel-2.5.2.26539-14.4.1  
libfbclient2-2.5.2.26539-14.4.1  
firebird-debugsource-2.5.2.26539-14.4.1  
firebird-2.5.2.26539-14.4.1  
libfbclient2-debuginfo-2.5.2.26539-14.4.1  
libfbclient2-devel-2.5.2.26539-14.4.1  
libfbembed2\_5-2.5.2.26539-14.4.1

## 170438 - Amazon Linux AMI ALAS-2014-460 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8088, CVE-2014-8089

### Description

The scan detected that the host is missing the following update:  
ALAS-2014-460

### Observation

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

<https://alas.aws.amazon.com/ALAS-2014-460.html>

Amazon Linux AMI

noarch

php-ZendFramework-Services-1.12.9-1.10.amzn1  
php-ZendFramework-Serializer-Adapter-Igbinary-1.12.9-1.10.amzn1  
php-ZendFramework-Captcha-1.12.9-1.10.amzn1  
php-ZendFramework-full-1.12.9-1.10.amzn1  
php-ZendFramework-Ldap-1.12.9-1.10.amzn1  
php-ZendFramework-Search-Lucene-1.12.9-1.10.amzn1  
php-ZendFramework-Cache-Backend-Apc-1.12.9-1.10.amzn1  
php-ZendFramework-extras-1.12.9-1.10.amzn1  
php-ZendFramework-Db-Adapter-Pdo-1.12.9-1.10.amzn1  
php-ZendFramework-Cache-Backend-Memcached-1.12.9-1.10.amzn1  
php-ZendFramework-Db-Adapter-Mysqli-1.12.9-1.10.amzn1  
php-ZendFramework-1.12.9-1.10.amzn1  
php-ZendFramework-Soap-1.12.9-1.10.amzn1  
php-ZendFramework-Dojo-1.12.9-1.10.amzn1  
php-ZendFramework-Cache-Backend-Libmemcached-1.12.9-1.10.amzn1  
php-ZendFramework-Auth-Adapter-Ldap-1.12.9-1.10.amzn1  
php-ZendFramework-Feed-1.12.9-1.10.amzn1  
php-ZendFramework-Db-Adapter-Pdo-Mssql-1.12.9-1.10.amzn1  
php-ZendFramework-Db-Adapter-Pdo-Pgsql-1.12.9-1.10.amzn1  
php-ZendFramework-demos-1.12.9-1.10.amzn1  
php-ZendFramework-Pdf-1.12.9-1.10.amzn1  
php-ZendFramework-Db-Adapter-Pdo-Mysql-1.12.9-1.10.amzn1

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

Risk Level: Medium

CVE: CVE-2004-2771, CVE-2014-7844

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Moderate: mailx on SL6.x, SL7.x i386/x86\_64 (1412-2833)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1412&L=scientific-linux-errata&T=0&P=2833>

SL7

x86\_64

mailx-debuginfo-12.5-12.el7\_0

mailx-12.5-12.el7\_0

SL6

x86\_64

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

i386

mailx-debuginfo-12.4-8.el6\_6

mailx-12.4-8.el6\_6

### **178003 - Gentoo Linux GLSA-201412-30 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2013-0345, CVE-2013-4484

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-30

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-30.xml>

Affected packages:

www-servers/varnish < 3.0.5

### **178016 - Gentoo Linux GLSA-201412-16 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-2668

#### Description

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



GLSA-201412-16

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-16.xml>

Affected packages:

dev-db/couchdb < 1.5.1

## **178020 - Gentoo Linux GLSA-201412-06 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3660

### Description

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

GLSA-201412-06

### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-06.xml>

Affected packages:

dev-libs/libxml2 < 2.9.2

## **184644 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2440-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-9116

### Description

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

USN-2440-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002761.html>

Ubuntu 14.10

mutt-patched\_1.5.23-1.1ubuntu0.2

mutt\_1.5.23-1.1ubuntu0.2

Ubuntu 14.04

mutt\_1.5.21-6.4ubuntu2.1

mutt-patched\_1.5.21-6.4ubuntu2.1

Ubuntu 12.04

mutt\_1.5.21-5ubuntu2.2  
mutt-patched\_1.5.21-5ubuntu2.2

Ubuntu 10.04

mutt\_1.5.20-7ubuntu1.3  
mutt-patched\_1.5.20-7ubuntu1.3

### 188615 - Fedora Linux 21 FEDORA-2014-16073 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16073

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146025.html>

Fedora Core 21

libyaml-0.1.6-6.fc21

### 188617 - Fedora Linux 20 FEDORA-2014-16132 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16132

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146130.html>

Fedora Core 20

libyaml-0.1.6-2.fc20

### 188618 - Fedora Linux 19 FEDORA-2014-16130 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16130

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146084.html>

Fedora Core 19

libyaml-0.1.6-2.fc19

### **188625 - Fedora Linux 21 FEDORA-2014-16435 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-9018, CVE-2014-9091

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16435

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146262.html>

Fedora Core 21

icecast-2.4.1-1.fc21

### **188626 - Fedora Linux 21 FEDORA-2014-16327 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-9218, CVE-2014-9219

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16327

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145804.html>

Fedora Core 21

phpMyAdmin-4.2.13.1-1.fc21

## 188627 - Fedora Linux 19 FEDORA-2014-16474 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9218, CVE-2014-9219

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16474

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146194.html>

Fedora Core 19

phpMyAdmin-4.2.13.1-1.fc19

## 188630 - Fedora Linux 20 FEDORA-2014-16266 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16266

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146122.html>

Fedora Core 20

perl-YAML-LibYAML-0.54-1.fc20

## 188632 - Fedora Linux 21 FEDORA-2014-16163 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8123

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16163

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145756.html>

Fedora Core 21

antiword-0.37-17.fc21

### 188634 - Fedora Linux 20 FEDORA-2014-16394 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9018, CVE-2014-9091

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16394

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146260.html>

Fedora Core 20

icecast-2.4.1-1.fc20

### 188639 - Fedora Linux 21 FEDORA-2014-16312 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0363

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16312

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145995.html>

Fedora Core 21

smack-3.2.2-8.fc21

### 188641 - Fedora Linux 19 FEDORA-2014-16210 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

## Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16210

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145996.html>

Fedora Core 19

perl-YAML-LibYAML-0.54-1.fc19

## 188643 - Fedora Linux 20 FEDORA-2014-16358 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9218, CVE-2014-9219

## Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16358

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145885.html>

Fedora Core 20

phpMyAdmin-4.2.13.1-1.fc20

## 188647 - Fedora Linux 19 FEDORA-2014-16257 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8123

## Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16257

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146149.html>

Fedora Core 19

antiword-0.37-17.fc19

## 188649 - Fedora Linux 21 FEDORA-2014-15573 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8964

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15573

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145843.html>

Fedora Core 21

pcre-8.35-8.fc21

## 188654 - Fedora Linux 20 FEDORA-2014-16241 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8123

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16241

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146178.html>

Fedora Core 20

antiword-0.37-17.fc20

## 188655 - Fedora Linux 21 FEDORA-2014-16143 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9130

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16143

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145949.html>

Fedora Core 21

perl-YAML-LibYAML-0.54-1.fc21

### **188658 - Fedora Linux 19 FEDORA-2014-16483 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-9018, CVE-2014-9091

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16483

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146204.html>

Fedora Core 19

icecast-2.4.1-1.fc19

### **188660 - Fedora Linux 20 FEDORA-2014-16383 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-0363

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16383

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146206.html>

Fedora Core 20

smack-3.2.2-6.fc20

### **17446 - IBM WebSphere Application Server Java Multiple Vulnerabilities (October 2014 CPU)**

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

Risk Level: Medium

CVE: CVE-2014-3566, CVE-2014-6457, CVE-2014-6512, CVE-2014-6558

#### Description



Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

#### Observation

IBM WebSphere Application Server is a Java application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in IBM Java SDK. Successful exploitation could allow an attacker to cause unknown impact or conduct a man-in-the-middle attack.

### **17515 - Microsoft Windows "xxxMenuWindowProc()" Denial of Service Vulnerability**

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Description

A denial of service vulnerability is present in some versions of Microsoft Windows.

#### Observation

The Windows kernel is the core of the Windows operating system.

A denial of service vulnerability is present in some versions of Microsoft Windows. The flaw lies in the "xxxMenuWindowProc()" function (win32k.sys). Successful exploitation could allow a denial of service condition.

### **17538 - IBM WebSphere Portal Cross-Site Scripting Vulnerability**

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

Risk Level: Medium

CVE: CVE-2014-6215

#### Description

A vulnerability is present in some versions of IBM WebSphere Portal.

#### Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A vulnerability is present in some versions of IBM WebSphere Portal. The flaw is due to improper validation of user-supplied input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

### **130027 - Debian Linux 7.0 DSA-3097-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8602

#### Description

The scan detected that the host is missing the following update:  
DSA-3097-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3097>

Debian 7.0  
all  
unbound\_1.4.17-3+deb7u2

### 178004 - Gentoo Linux GLSA-201412-20 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes  
Risk Level: Medium  
CVE: CVE-2014-2980

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-20

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-20.xml>

Affected packages:  
gnustep-base/gnustep-base < 1.24.6-r1

### 178008 - Gentoo Linux GLSA-201412-25 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes  
Risk Level: Medium  
CVE: CVE-2014-0190

#### Description

The scan detected that the host is missing the following update:  
GLSA-201412-25

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201412-25.xml>

Affected packages:  
dev-qt/qtgui < 4.8.5-r2

### 188623 - Fedora Linux 20 FEDORA-2014-16632 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16632

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146138.html>

Fedora Core 20

kernel-3.17.6-200.fc20

### **188624 - Fedora Linux 20 FEDORA-2014-16538 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3707

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16538

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146090.html>

Fedora Core 20

curl-7.32.0-17.fc20

### **188645 - Fedora Linux 21 FEDORA-2014-15967 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2010-5312

### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15967

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145821.html>

Fedora Core 21

couchdb-1.6.1-4.fc21

### **188652 - Fedora Linux 20 FEDORA-2014-16346 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3004

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16346

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146251.html>

Fedora Core 20

castor-1.3.3-1.fc20

### **188653 - Fedora Linux 19 FEDORA-2014-15390 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-3566

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15390

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146244.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146243.html>

Fedora Core 19

libuv-0.10.29-1.fc19

nodejs-0.10.33-1.fc19

### **188657 - Fedora Linux 20 FEDORA-2014-16048 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2010-5312

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16048

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145767.html>

Fedora Core 20

### 188659 - Fedora Linux 21 FEDORA-2014-16605 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3707

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16605

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146193.html>

Fedora Core 21

curl-7.37.0-11.fc21

### 188664 - Fedora Linux 21 FEDORA-2014-16446 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3004

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16446

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146246.html>

Fedora Core 21

castor-1.3.3-1.fc21

### 188665 - Fedora Linux 21 FEDORA-2014-15411 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15411

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146220.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146221.html>

Fedora Core 21

libuv-0.10.29-1.fc21  
nodejs-0.10.33-1.fc21

### 188666 - Fedora Linux 20 FEDORA-2014-15379 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3566

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15379

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146233.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146232.html>

Fedora Core 20

nodejs-0.10.33-1.fc20  
libuv-0.10.29-1.fc20

### 188670 - Fedora Linux 21 FEDORA-2014-16448 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-9090

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16448

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145786.html>

Fedora Core 21

kernel-3.17.4-302.fc21

### 55238 - Top Weekly Malware Env - Trojan-2f1f76cf (2f1f76cf.exe)

Category: Windows Host Assessment -> Top Weekly Malware  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is infected by the malware:

Env - Trojan-2f1f76cf (2f1f76cf.exe)

#### Observation

This malware shows the following behavior:

The files and directories below were created:

%temp%\2f1f76cf.exe

For more information on this malware, visit <http://vil.nai.com/vil/default.aspx>

### **88652 - Slackware Linux 14.0, 14.1 SSA:2014-344-06 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

SSA:2014-344-06

#### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.490951>

Slackware 14.1

x86\_64

seamoney-solibs-2.31-x86\_64-1

seamoney-2.31-x86\_64-1

Slackware 14.0

x86\_64

seamoney-solibs-2.31-x86\_64-1

seamoney-2.31-x86\_64-1

### **88653 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2014-344-05 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

SSA:2014-344-05

#### Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.487293>

Slackware 13.0  
x86\_64  
pidgin-2.10.11-x86\_64-1

Slackware 14.1  
x86\_64  
pidgin-2.10.11-x86\_64-1

Slackware 13.37  
x86\_64  
pidgin-2.10.11-x86\_64-1

Slackware 13.1  
x86\_64  
pidgin-2.10.11-x86\_64-1

Slackware 14.0  
x86\_64  
pidgin-2.10.11-x86\_64-1

#### **88654 - Slackware Linux 14.0, 14.1 SSA:2014-344-03 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
SSA:2014-344-03

#### Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.377012>

Slackware 14.1  
x86\_64  
openssh-6.7p1-x86\_64-2

Slackware 14.0  
x86\_64  
openssh-6.7p1-x86\_64-2

#### **88655 - Slackware Linux 14.1 SSA:2014-344-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description



The scan detected that the host is missing the following update:  
SSA:2014-344-02

#### Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2014&m=slackware-security.311336>

Slackware 14.1  
x86\_64  
mozilla-firefox-31.3.0esr-x86\_64-1

### **93437 - Mandriva Linux MBS1 MDVSA-2014-241 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-9276, CVE-2014-9277

#### Description

The scan detected that the host is missing the following update:  
MDVSA-2014-241

#### Observation

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

<https://www.mandriva.com/en/support/security/advisories/mbs1/MDVSA-2014%3A241/>

Mandriva Linux mbs1  
x86\_64  
mediawiki-pgsql-1.23.7-1  
mediawiki-mysql-1.23.7-1  
mediawiki-sqlite-1.23.7-1  
mediawiki-1.23.7-1

### **130020 - Debian Linux 7.0 DSA-3101-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2013-7401, CVE-2013-7402

#### Description

The scan detected that the host is missing the following update:  
DSA-3101-1

#### Observation

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

<http://www.debian.org/security/2014/dsa-3101>

Debian 7.0  
all  
c-icap\_1:0.1.6-1.1+deb7u1

## 130021 - Debian Linux 7.0 DSA-3100-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9277

### Description

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

DSA-3100-1

### Observation

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

For more information see:

<http://www.debian.org/security/2014/dsa-3100>

Debian 7.0

all

mediawiki\_1:1.19.20+dfsg-0+deb7u2

## 142558 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1637-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9092

### Description

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

openSUSE-SU-2014:1637-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00055.html>

SuSE Linux 13.1

x86\_64

libjpeg8-debuginfo-32bit-8.0.2-24.4.1

libjpeg8-devel-32bit-8.0.2-24.4.1

libjpeg8-32bit-8.0.2-24.4.1

libjpeg62-debuginfo-32bit-62.0.0-24.4.1

libjpeg62-devel-32bit-62.0.0-24.4.1

libjpeg62-32bit-62.0.0-24.4.1

i586

libjpeg8-devel-8.0.2-24.4.1

libjpeg62-62.0.0-24.4.1

libjpeg62-turbo-debugsource-1.2.1-24.4.1

libjpeg62-debuginfo-62.0.0-24.4.1

libjpeg62-devel-62.0.0-24.4.1

libjpeg8-debuginfo-8.0.2-24.4.1

libjpeg-turbo-1.2.1-24.4.1

libjpeg-turbo-debuginfo-1.2.1-24.4.1

libjpeg8-8.0.2-24.4.1

libjpeg-turbo-debugsource-1.2.1-24.4.1  
libjpeg62-turbo-1.2.1-24.4.1

SuSE Linux 12.3

x86\_64  
libjpeg62-32bit-62.0.0-19.20.1  
libjpeg8-devel-32bit-8.0.2-19.20.1  
libjpeg62-debuginfo-32bit-62.0.0-19.20.1  
libjpeg62-devel-32bit-62.0.0-19.20.1  
libjpeg8-32bit-8.0.2-19.20.1  
libjpeg8-debuginfo-32bit-8.0.2-19.20.1

i586

libjpeg-turbo-debuginfo-1.2.1-19.20.1  
libjpeg62-turbo-1.2.1-19.20.1  
libjpeg8-debuginfo-8.0.2-19.20.1  
libjpeg62-debuginfo-62.0.0-19.20.1  
libjpeg62-62.0.0-19.20.1  
libjpeg62-turbo-debugsource-1.2.1-19.20.1  
libjpeg-turbo-debugsource-1.2.1-19.20.1  
libjpeg62-devel-62.0.0-19.20.1  
libjpeg-turbo-1.2.1-19.20.1  
libjpeg8-8.0.2-19.20.1  
libjpeg8-devel-8.0.2-19.20.1

SuSE Linux 13.2

x86\_64  
libjpeg8-32bit-8.0.2-30.5.1  
libjpeg62-32bit-62.1.0-30.5.1  
libjpeg8-debuginfo-32bit-8.0.2-30.5.1  
libjpeg62-devel-32bit-62.1.0-30.5.1  
libturbojpeg0-debuginfo-32bit-8.0.2-30.5.1  
libturbojpeg0-32bit-8.0.2-30.5.1  
libjpeg62-debuginfo-32bit-62.1.0-30.5.1  
libjpeg8-devel-32bit-8.0.2-30.5.1

i586

libjpeg62-turbo-1.3.1-30.5.1  
libjpeg-turbo-debuginfo-1.3.1-30.5.1  
libjpeg8-devel-8.0.2-30.5.1  
libjpeg8-8.0.2-30.5.1  
libturbojpeg0-debuginfo-8.0.2-30.5.1  
libjpeg-turbo-1.3.1-30.5.1  
libjpeg-turbo-debugsource-1.3.1-30.5.1  
libjpeg8-debuginfo-8.0.2-30.5.1  
libturbojpeg0-8.0.2-30.5.1  
libjpeg62-debuginfo-62.1.0-30.5.1  
libjpeg62-turbo-debugsource-1.3.1-30.5.1  
libjpeg62-62.1.0-30.5.1  
libjpeg62-devel-62.1.0-30.5.1

### 142560 - SuSE SLES 11 SP3, SLED 11 SP3 ImageMagick-9976 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716

#### Description

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

ImageMagick-9976

### Observation

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

<https://download.suse.com/Download?buildid=dZUbdOkPHt0~>  
[https://download.suse.com/Download?buildid=Cow20L\\_DaPI~](https://download.suse.com/Download?buildid=Cow20L_DaPI~)  
<https://download.suse.com/Download?buildid=xREy1svNPeo~>  
[https://download.suse.com/Download?buildid=Hug8d\\_UFFHA~](https://download.suse.com/Download?buildid=Hug8d_UFFHA~)  
<https://download.suse.com/Download?buildid=JpcSrlr5IGc~>  
<https://download.suse.com/Download?buildid=JSs8X97eHRo~>  
<https://download.suse.com/Download?buildid=MXBiWK2r45k~>  
<https://download.suse.com/Download?buildid=Cg3HETGWkEQ~>  
<https://download.suse.com/Download?buildid=AtnEyvQ1CLw~>

SuSE SLED 11 SP3

x86\_64

ImageMagick-6.4.3.6-7.30.1

libMagickCore1-6.4.3.6-7.30.1

libMagickWand1-6.4.3.6-7.30.1

libMagickCore1-32bit-6.4.3.6-7.30.1

libMagick++1-6.4.3.6-7.30.1

i586

ImageMagick-6.4.3.6-7.30.1

libMagickCore1-6.4.3.6-7.30.1

libMagickWand1-6.4.3.6-7.30.1

libMagick++1-6.4.3.6-7.30.1

SuSE SLES 11 SP3

x86\_64

libMagickCore1-6.4.3.6-7.30.1

libMagickCore1-32bit-6.4.3.6-7.30.1

i586

libMagickCore1-6.4.3.6-7.30.1

## **142571 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1646-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2013-2131

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2014:1646-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2014-12/msg00064.html>

SuSE Linux 13.1

i586

ruby-rrdtool-debuginfo-1.4.7-13.4.1

ruby-rrdtool-1.4.7-13.4.1  
rrdtool-devel-1.4.7-13.4.1  
python-rrdtool-debuginfo-1.4.7-13.4.1  
rrdtool-debuginfo-1.4.7-13.4.1  
lua-rrdtool-1.4.7-13.4.1  
rrdtool-debugsource-1.4.7-13.4.1  
python-rrdtool-1.4.7-13.4.1  
rrdtool-1.4.7-13.4.1  
tcl-rrdtool-debuginfo-1.4.7-13.4.1  
lua-rrdtool-debuginfo-1.4.7-13.4.1  
tcl-rrdtool-1.4.7-13.4.1

SuSE Linux 12.3

i586

python-rrdtool-debuginfo-1.4.7-8.4.1  
lua-rrdtool-debuginfo-1.4.7-8.4.1  
tcl-rrdtool-debuginfo-1.4.7-8.4.1  
lua-rrdtool-1.4.7-8.4.1  
tcl-rrdtool-1.4.7-8.4.1  
rrdtool-devel-1.4.7-8.4.1  
rrdtool-debuginfo-1.4.7-8.4.1  
rrdtool-debugsource-1.4.7-8.4.1  
python-rrdtool-1.4.7-8.4.1  
rrdtool-1.4.7-8.4.1

SuSE Linux 13.2

i586

rrdtool-debugsource-1.4.7-20.4.1  
rrdtool-1.4.7-20.4.1  
ruby-rrdtool-1.4.7-20.4.1  
tcl-rrdtool-1.4.7-20.4.1  
lua-rrdtool-debuginfo-1.4.7-20.4.1  
python-rrdtool-1.4.7-20.4.1  
python-rrdtool-debuginfo-1.4.7-20.4.1  
rrdtool-cached-debuginfo-1.4.7-20.4.1  
rrdtool-devel-1.4.7-20.4.1  
tcl-rrdtool-debuginfo-1.4.7-20.4.1  
rrdtool-cached-1.4.7-20.4.1  
lua-rrdtool-1.4.7-20.4.1  
rrdtool-debuginfo-1.4.7-20.4.1  
ruby-rrdtool-debuginfo-1.4.7-20.4.1

### 181300 - FreeBSD subversion DoS Vulnerabilities (f5561ade-846c-11e4-b7a7-20cf30e32f6d)

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

Risk Level: Low

CVE: CVE-2014-3580, CVE-2014-8108

#### Description

The scan detected that the host is missing the following update:  
subversion -- DoS vulnerabilities (f5561ade-846c-11e4-b7a7-20cf30e32f6d)

#### Observation

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

<http://www.vuxml.org/freebsd/f5561ade-846c-11e4-b7a7-20cf30e32f6d.html>

Affected packages:

1.8.0 <= mod\_dav\_svn < 1.8.11

1.0.0 <= subversion16 < 1.7.19

1.0.0 <= subversion17 < 1.7.19

1.0.0 <= subversion < 1.7.19

1.8.0 <= subversion < 1.8.11

### **181302 - FreeBSD asterisk Remote Crash Vulnerability In WebSocket Server (94268da0-8118-11e4-a180-001999f8d30b)**

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:

asterisk -- Remote Crash Vulnerability in WebSocket Server (94268da0-8118-11e4-a180-001999f8d30b)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/94268da0-8118-11e4-a180-001999f8d30b.html>

Affected packages:

asterisk11 < 11.14.2

### **181304 - FreeBSD otrs Incomplete Access Control (0c5cf7c4-856e-11e4-a089-60a44c524f57)**

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

Risk Level: Low

CVE: CVE-2014-9324

#### Description

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

otrs -- Incomplete Access Control (0c5cf7c4-856e-11e4-a089-60a44c524f57)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/0c5cf7c4-856e-11e4-a089-60a44c524f57.html>

Affected packages:

3.2.\* < otrs < 3.2.17

3.3.\* < otrs < 3.3.11

4.0.\* < otrs < 4.0.3

### **184642 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2436-2 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
USN-2436-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2014-December/002758.html>

Ubuntu 14.10

xserver-xorg-core\_1.16.0-1ubuntu1.2

Ubuntu 14.04

xserver-xorg-core\_1.15.1-0ubuntu2.5

Ubuntu 12.04

xserver-xorg-core-lts-trusty\_1.15.1-0ubuntu2~precise4

xserver-xorg-core\_1.11.4-0ubuntu10.16

### **188616 - Fedora Linux 20 FEDORA-2014-16378 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-4607

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16378

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145948.html>

Fedora Core 20

grub2-2.00-27.fc20

### **188628 - Fedora Linux 20 FEDORA-2014-16368 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2013-4440, CVE-2013-4442

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16368

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146015.html>

Fedora Core 20

pwgen-2.07-1.fc20

#### **188629 - Fedora Linux 20 FEDORA-2014-16262 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-2014-16262

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146024.html>

Fedora Core 20

kde-plasma-nm-0.9.3.5-2.fc20

#### **188635 - Fedora Linux 20 FEDORA-2014-16397 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-2014-16397

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146258.html>

Fedora Core 20

php-horde-kronolith-4.2.4-1.fc20

#### **188638 - Fedora Linux 21 FEDORA-2014-16623 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-2014-16623

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146231.html>

Fedora Core 21

xorg-x11-server-1.16.2.901-1.fc21

### **188640 - Fedora Linux 21 FEDORA-2014-16318 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-2014-16318

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146116.html>

Fedora Core 21

kde-plasma-nm-0.9.3.5-2.fc21

### **188648 - Fedora Linux 19 FEDORA-2014-16017 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-2014-16017

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145984.html>

Fedora Core 19

xen-4.2.5-6.fc19

### **188661 - Fedora Linux 21 FEDORA-2014-16406 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2013-4440, CVE-2013-4442

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16406

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146237.html>

Fedora Core 21

pwgen-2.07-1.fc21

### **188662 - Fedora Linux 21 FEDORA-2014-16403 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-4607

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-16403

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145905.html>

Fedora Core 21

grub2-2.02-0.13.fc21

### **188663 - Fedora Linux 21 FEDORA-2014-15908 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-9114

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2014-15908

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146229.html>

Fedora Core 21

util-linux-2.25.2-2.fc21

### 188667 - Fedora Linux 21 FEDORA-2014-15621 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-2014-15621

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145942.html>

Fedora Core 21

asterisk-11.14.1-1.fc21

### 188669 - Fedora Linux 20 FEDORA-2014-15995 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-2014-15995

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/145940.html>

Fedora Core 20

xen-4.3.3-6.fc20

### 188671 - Fedora Linux 19 FEDORA-2014-16203 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-2014-16203

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146111.html>

Fedora Core 19

kde-plasma-networkmanagement-0.9.0.11-2.fc19

### **188674 - Fedora Linux 21 FEDORA-2014-16329 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-2014-16329

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2014-December/146103.html>

Fedora Core 21

php-horde-kronolith-4.2.4-1.fc21

### **17467 - Google Android 'handleSmsSent()' Function Information Disclosure Vulnerability**

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: Low

CVE: CVE-2014-8610

#### Description

An information disclosure vulnerability is present in some versions of Google Android.

#### Observation

Google Android is a popular mobile operating system.

An information disclosure vulnerability is present in some versions of Google Android. The flaw lies in handleSmsSent function. Successful exploitation could allow an attacker to obtain victim's SMS content.

### **130023 - Debian Linux 7.0 DSA-3099-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-7824

#### Description

The scan detected that the host is missing the following update:  
DSA-3099-1

### Observation

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

<http://www.debian.org/security/2014/dsa-3099>

Debian 7.0  
all  
dbus\_1.6.8-1+deb7u5

### **33285 - Oracle Solaris 151074-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-3956

### Description

The scan detected that the host is missing the following update:  
151074-02

### Observation

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

<https://getupdates.oracle.com/readme/151074-02>

SunOS 5.10: sendmail patch

SOLARIS\_10

SUNWsndmu:11.10.0,REV=2005.01.21.15.53  
SUNWsndmr:11.10.0,REV=2005.01.21.15.53

### **33286 - Oracle Solaris 151075-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2014-3956

### Description

The scan detected that the host is missing the following update:  
151075-02

### Observation

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

<https://getupdates.oracle.com/readme/151075-02>

SunOS 5.10(x86): sendmail patch

SOLARIS\_10\_x86

SUNWsndmr:11.10.0,REV=2005.01.21.16.34  
SUNWsndmu:11.10.0,REV=2005.01.21.16.34

## 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.

### 17225 - (MS14-057) Microsoft .NET Framework Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4121

[Update Details](#)

Risk is updated

### 17226 - (MS14-057) Microsoft .NET Framework ClickOnce Privilege Escalation (3000414)

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

Risk Level: High

CVE: CVE-2014-4073

[Update Details](#)

Risk is updated

### 17360 - (MS14-066) Microsoft Windows Schannel Remote Code Execution (2992611)

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

Risk Level: High

CVE: CVE-2014-6321

[Update Details](#)

Risk is updated

### 17517 - (APSB14-27) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

[Update Details](#)

Risk is updated

### 17518 - (APSB14-27) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

[Update Details](#)

Risk is updated

### 33275 - Oracle Solaris 149079-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

#### Update Details

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

### 33276 - Oracle Solaris 149080-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

#### Update Details

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

### 33277 - Oracle Solaris 150512-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

#### Update Details

CVE is updated

### 33278 - Oracle Solaris 150513-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-3410, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

#### Update Details

CVE is updated

### 140636 - Red Hat Enterprise Linux RHSA-2014-1976 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

#### Update Details

Risk is updated

### 170432 - Amazon Linux AMI ALAS-2014-458 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6435, CVE-2014-8118

[Update Details](#)

Risk is updated

**16993 - Apple QuickTime mvhd Atom Remote Code Execution**

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

Risk Level: High

CVE: CVE-2014-4979

[Update Details](#)

Recommendation is updated

**17002 - (MS14-048) Microsoft OneNote File Parsing Remote Code Execution (2977201)**

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

Risk Level: High

CVE: CVE-2014-2815

[Update Details](#)

Risk is updated

**17004 - (MS14-050) Microsoft Sharepoint Server Page Content Privilege Escalation (2977202)**

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

Risk Level: High

CVE: CVE-2014-2816

[Update Details](#)

Risk is updated

**17005 - (MS14-050) Vulnerability in Microsoft SharePoint Server Could Allow Elevation of Privilege (2977202)**

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

Risk Level: High

CVE: CVE-2014-2816

[Update Details](#)

Risk is updated

**17009 - (MS14-048) Vulnerability in OneNote Could Allow Remote Code Execution (2977201)**

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

Risk Level: High

CVE: CVE-2014-2815



[Update Details](#)

Risk is updated

**17101 - (MS14-052) Cumulative Security Update for Internet Explorer (2977629)**

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

Risk Level: High

CVE: CVE-2013-7331, CVE-2014-4082, CVE-2014-4083, CVE-2014-4084, CVE-2014-4085, CVE-2014-4086, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089, CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094, CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099, CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, CVE-2014-4111

[Update Details](#)

Risk is updated

**17159 - (VMSA-2014-0008) VMware vCenter Server Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-4322, CVE-2013-4590, CVE-2013-6629, CVE-2013-6954, CVE-2014-0050, CVE-2014-0114, CVE-2014-0429, CVE-2014-0432, CVE-2014-0446, CVE-2014-0448, CVE-2014-0449, CVE-2014-0451, CVE-2014-0452, CVE-2014-0453, CVE-2014-0454, CVE-2014-0455, CVE-2014-0456, CVE-2014-0457, CVE-2014-0458, CVE-2014-0459, CVE-2014-0460, CVE-2014-0461, CVE-2014-1876, CVE-2014-2397, CVE-2014-2398, CVE-2014-2401, CVE-2014-2402, CVE-2014-2403, CVE-2014-2409, CVE-2014-2412, CVE-2014-2413, CVE-2014-2414, CVE-2014-2420, CVE-2014-2421, CVE-2014-2422, CVE-2014-2423, CVE-2014-2427, CVE-2014-2428

[Update Details](#)

FASLScript is updated

**17160 - (VMSA-2014-0008) VMware vCenter Server Multiple Vulnerabilities**

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

Risk Level: High

CVE: CVE-2013-4322, CVE-2013-4590, CVE-2013-6629, CVE-2013-6954, CVE-2014-0050, CVE-2014-0114, CVE-2014-0429, CVE-2014-0432, CVE-2014-0446, CVE-2014-0448, CVE-2014-0449, CVE-2014-0451, CVE-2014-0452, CVE-2014-0453, CVE-2014-0454, CVE-2014-0455, CVE-2014-0456, CVE-2014-0457, CVE-2014-0458, CVE-2014-0459, CVE-2014-0460, CVE-2014-0461, CVE-2014-1876, CVE-2014-2397, CVE-2014-2398, CVE-2014-2401, CVE-2014-2402, CVE-2014-2403, CVE-2014-2409, CVE-2014-2412, CVE-2014-2413, CVE-2014-2414, CVE-2014-2420, CVE-2014-2421, CVE-2014-2422, CVE-2014-2423, CVE-2014-2427, CVE-2014-2428

[Update Details](#)

FASLScript is updated

**17227 - (MS14-058) Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)**

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

Risk Level: High

CVE: CVE-2014-4113, CVE-2014-4148

[Update Details](#)

Risk is updated

#### 17246 - (MS14-060) Microsoft Windows OLE Remote Code Execution (3000869)

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

Risk Level: High

CVE: CVE-2014-4114

[Update Details](#)

Risk is updated

#### 17258 - (MS14-061) Microsoft Word File Format Remote Code Execution (3000434)

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

Risk Level: High

CVE: CVE-2014-4117

[Update Details](#)

Risk is updated

#### 17363 - (MS14-064) Microsoft Windows OLE Automation Array Remote Code Execution (3011443)

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

Risk Level: High

CVE: CVE-2014-6332

[Update Details](#)

Risk is updated

#### 17364 - (MS14-064) Microsoft Windows OLE Remote Code Execution (3011443)

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

Risk Level: High

CVE: CVE-2014-6352

[Update Details](#)

Risk is updated

#### 17386 - (MS14-069) Microsoft Word Invalid Pointer Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6335

[Update Details](#)

Risk is updated

#### 17387 - (MS14-069) Microsoft Word Bad Index Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6334

[Update Details](#)

Risk is updated

#### **17388 - (MS14-069) Microsoft Word Double Delete Remote Code Execution (3009710)**

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

Risk Level: High

CVE: CVE-2014-6333

[Update Details](#)

Risk is updated

#### **17396 - (MS14-072) Microsoft .NET Framework Remoting TypeFilterLevel Privilege Escalation (3005210)**

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

Risk Level: High

CVE: CVE-2014-4149

[Update Details](#)

Risk is updated

#### **17397 - (MS14-078) Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)**

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

Risk Level: High

CVE: CVE-2014-4077

[Update Details](#)

Risk is updated

#### **17398 - (MS14-078) Microsoft Windows IME (Japanese) Privilege Escalation (2992719)**

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

Risk Level: High

CVE: CVE-2014-4077

[Update Details](#)

Risk is updated

#### **17483 - (MS14-082) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3017349)**

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

Risk Level: High  
CVE: CVE-2014-6364

Update Details

Risk is updated

**17485 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)**

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

Risk Level: High  
CVE: CVE-2014-6356 , CVE-2014-6357

Update Details

Name is updated Risk is updated

**17486 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High  
CVE: CVE-2014-6356 , CVE-2014-6357

Update Details

Name is updated Risk is updated

**17487 - (MS14-083) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)**

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

Risk Level: High  
CVE: CVE-2014-6360 , CVE-2014-6361

Update Details

Risk is updated

**17490 - (MS14-083) Microsoft Excel Global Free Remote Code Execution (3017347)**

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

Risk Level: High  
CVE: CVE-2014-6360

Update Details

Risk is updated

**17491 - (MS14-083) Microsoft Excel Excel Invalid Pointer Remote Code Execution (3017347)**

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

Risk Level: High

CVE: CVE-2014-6361

[Update Details](#)

Risk is updated

**17494 - (MS14-082) Microsoft Office Component Use-After-Free Remote Code Execution (3017349)**

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

Risk Level: High

CVE: CVE-2014-6364

[Update Details](#)

Risk is updated

**43150 - HP-UX 11.X PHCO\_43875 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-7879

[Update Details](#)

Risk is updated

**43151 - HP-UX 11.X PHCO\_43873 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-7879

[Update Details](#)

Risk is updated

**43153 - HP-UX 11.X PHCO\_43874 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-7879

[Update Details](#)

Risk is updated

**16964 - (MS14-047) Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)**

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

Risk Level: High

CVE: CVE-2014-0316

[Update Details](#)

Risk is updated

### 16965 - (MS14-047) Microsoft Windows ASLR Bypass Security Bypass (2978668)

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

Risk Level: High

CVE: CVE-2014-0316

[Update Details](#)

Risk is updated

### 16998 - (MS14-045) Microsoft Windows Font Double-Fetch Privilege Escalation (2984615)

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

Risk Level: High

CVE: CVE-2014-1819

[Update Details](#)

Risk is updated

### 17000 - (MS14-045) Microsoft Windows Win32k Privilege Escalation (2984615)

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

Risk Level: High

CVE: CVE-2014-0318

[Update Details](#)

Risk is updated

### 17003 - (MS14-049) Microsoft Windows Installer Repair Privilege Escalation (2962490)

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

Risk Level: High

CVE: CVE-2014-1814

[Update Details](#)

Risk is updated

### 17008 - (MS14-049) Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (2962490)

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

Risk Level: High

CVE: CVE-2014-1814

[Update Details](#)

Risk is updated

### 17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

---

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

Risk Level: High

CVE: CVE-2014-4113

[Update Details](#)

Risk is updated

#### **17261 - (MS14-062) Microsoft Message Queuing Service Arbitrary Write Privilege Escalation (2993254)**

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

Risk Level: High

CVE: CVE-2014-4971

[Update Details](#)

Risk is updated

#### **17263 - (MS14-063) Microsoft Windows Disk Partition Driver Privilege Escalation (2998579)**

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

Risk Level: High

CVE: CVE-2014-4115

[Update Details](#)

Risk is updated

#### **17391 - (MS14-070) Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)**

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

Risk Level: High

CVE: CVE-2014-4076

[Update Details](#)

Risk is updated

#### **17392 - (MS14-070) Microsoft Windows TCP/IP IOCTL Privilege Escalation (2989935)**

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

Risk Level: High

CVE: CVE-2014-4076

[Update Details](#)

Risk is updated

#### **17409 - (MS14-079) Microsoft Windows Kernel Denial of Service (3002885)**

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

Risk Level: High  
CVE: CVE-2014-6317

[Update Details](#)

Risk is updated

**17453 - Google Android Local Privilege Escalation Vulnerability**

Category: Wireless Assessment -> NonIntrusive -> Android

Risk Level: High

CVE: CVE-2014-7911

[Update Details](#)

Risk is updated

**91676 - Oracle Enterprise Linux ELSA-2014-3095 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

[Update Details](#)

Risk is updated

**91678 - Oracle Enterprise Linux ELSA-2014-1974 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-6435

[Update Details](#)

FASLScript is updated

**130016 - Debian Linux 7.0 DSA-3094-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8500

[Update Details](#)

Risk is updated

**142546 - SuSE Linux 13.2 openSUSE-SU-2014:1596-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

[Update Details](#)

Risk is updated



### 170427 - Amazon Linux AMI ALAS-2014-454 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

#### Update Details

Risk is updated

### 184641 - Ubuntu Linux 10.04, 12.04, 14.04, 14.10 USN-2437-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500

#### Update Details

Risk is updated

### 188582 - Fedora Linux 21 FEDORA-2014-15779 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6407, CVE-2014-6408

#### Update Details

Risk is updated

### 14620 - DotNetNuke User Profile Images Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Update Details

Observation is updated

### 16959 - (MS14-043) Vulnerability in Windows Media Center Could Allow Remote Code Execution (2978742)

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

Risk Level: Medium

CVE: CVE-2014-4060

#### Update Details

Risk is updated

### 16963 - (MS14-044) Microsoft SQL Server Stack Overrun Privilege Escalation (2984340)

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

Risk Level: Medium

CVE: CVE-2014-4061

[Update Details](#)

Risk is updated

**16969 - (MS14-051) Microsoft Internet Explorer Privilege Escalation II (2976627)**

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

Risk Level: Medium

CVE: CVE-2014-2819

[Update Details](#)

Risk is updated

**16970 - (MS14-051) Microsoft Internet Explorer Privilege Escalation I (2976627)**

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

Risk Level: Medium

CVE: CVE-2014-2817

[Update Details](#)

Risk is updated

**17102 - (MS14-054) Microsoft Windows Task Scheduler Integrity Checks Privilege Escalation (2988948)**

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

Risk Level: Medium

CVE: CVE-2014-4074

[Update Details](#)

Risk is updated

**17103 - (MS14-054) Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (2988948)**

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

Risk Level: Medium

CVE: CVE-2014-4074

[Update Details](#)

Risk is updated

**17232 - (MS14-056) Microsoft Internet Explorer I Privilege Escalation (2987107)**

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

Risk Level: Medium

CVE: CVE-2014-4123

[Update Details](#)

Risk is updated

**17233 - (MS14-056) Microsoft Internet Explorer II Privilege Escalation (2987107)**

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

Risk Level: Medium

CVE: CVE-2014-4124

[Update Details](#)

Risk is updated

**17234 - (MS14-056) Microsoft Internet Explorer ASLR Security Bypass (2987107)**

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

Risk Level: Medium

CVE: CVE-2014-4140

[Update Details](#)

Risk is updated

**17347 - Nordex NC2 Cross-Site Scripting Vulnerability**

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2014-5408

[Update Details](#)

Recommendation is updated

**17511 - Microsoft Internet Explorer display:run-in Use After Free Remote Code Execution Vulnerability**

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

Risk Level: Medium

CVE: CVE-2014-8967

[Update Details](#)

Recommendation is updated Risk is updated

**85834 - CentOS 5, 6, 7 CESA-2014-1919 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **85837 - CentOS 5, 6 CESA-2014-1924 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **91679 - Oracle Enterprise Linux ELSA-2014-1924 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **91683 - Oracle Enterprise Linux ELSA-2014-1919 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **130013 - Debian Linux 7.0 DSA-3092-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **130018 - Debian Linux 7.0 DSA-3090-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

### **140624 - Red Hat Enterprise Linux RHSA-2014-1919 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

**140630 - Red Hat Enterprise Linux RHSA-2014-1924 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

**142540 - SuSE SLES 11 SP3, SLED 11 SP3 openvpn-10061 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8104

[Update Details](#)

FASLScript is updated

**142551 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:1590-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8583

[Update Details](#)

Risk is updated

**142555 - SuSE Linux 12.3, 13.1, 13.2 openSUSE-SU-2014:1581-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

**174601 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x i386/x86\_64 (1412-845)**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

**174604 - Scientific Linux Security ERRATA Critical: firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (1412-706)**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

#### **181299 - FreeBSD mozilla Multiple Vulnerabilities (7ae61870-9dd2-4884-a2f2-f19bb5784d09)**

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

Risk Level: Medium

CVE: CVE-2014-1569, CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595

[Update Details](#)

Risk is updated

#### **184626 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2424-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

#### **184635 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2428-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-1587, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594

[Update Details](#)

Risk is updated

#### **184638 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2431-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-8583

[Update Details](#)

Risk is updated

#### **17210 - GNU Bash read\_token\_word parse.y Denial of Service**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-7187

[Update Details](#)

FASLScript is updated

**17281 - SSLv3 Information Disclosure Vulnerability**

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

[Update Details](#)

Recommendation is updated FASLScript is updated

**16962 - (MS14-044) Microsoft SQL Server XSS Privilege Escalation (2984340)**

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

Risk Level: Medium

CVE: CVE-2014-1820

[Update Details](#)

Risk is updated

**16999 - (MS14-045) Microsoft Windows Kernel Pool Allocation Information Disclosure (2984615)**

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

Risk Level: Medium

CVE: CVE-2014-4064

[Update Details](#)

Risk is updated

**17001 - (MS14-046) Microsoft .NET Framework ASLR Security Bypass (2984625)**

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

Risk Level: Medium

CVE: CVE-2014-4062

[Update Details](#)

Risk is updated

**17010 - (MS14-046) Vulnerability in .NET Framework Could Allow Security Feature Bypass (2984625)**

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

Risk Level: Medium

CVE: CVE-2014-4062

[Update Details](#)

Risk is updated

**17109 - (MS14-055) Microsoft Lync Server Cross-Site Scripting Content Sanitizing Information Disclosure (2990928)**

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

Risk Level: Medium

CVE: CVE-2014-4070

[Update Details](#)

Risk is updated

**17224 - (MS14-057) Microsoft .NET Framework Address Space Layout Randomization Security Bypass (3000414)**

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

Risk Level: Medium

CVE: CVE-2014-4122

[Update Details](#)

Risk is updated

**17247 - (MS14-059) Microsoft ASP.NET MVC Feature Cross-Site Scripting (2990942)**

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

Risk Level: Medium

CVE: CVE-2014-4075

[Update Details](#)

Risk is updated

**17251 - (MS14-059) Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)**

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

Risk Level: Medium

CVE: CVE-2014-4075

[Update Details](#)

Risk is updated

**17367 - (MS14-065) Microsoft Internet Explorer Clipboard Information Disclosure (3003057)**

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

Risk Level: Medium

CVE: CVE-2014-6323

[Update Details](#)

Risk is updated

**17368 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure I (3003057)**



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

Risk Level: Medium

CVE: CVE-2014-6340

[Update Details](#)

Risk is updated

#### **17370 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure II (3003057)**

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

Risk Level: Medium

CVE: CVE-2014-6345

[Update Details](#)

Risk is updated

#### **17371 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure III (3003057)**

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

Risk Level: Medium

CVE: CVE-2014-6346

[Update Details](#)

Risk is updated

#### **17382 - (MS14-065) Microsoft Internet Explorer Permission Validation I Privilege Escalation (3003057)**

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

Risk Level: Medium

CVE: CVE-2014-6349

[Update Details](#)

Risk is updated

#### **17383 - (MS14-065) Microsoft Internet Explorer Permission Validation II Privilege Escalation (3003057)**

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

Risk Level: Medium

CVE: CVE-2014-6350

[Update Details](#)

Risk is updated

#### **17390 - (MS14-071) Microsoft Windows Audio Services Privilege Escalation (3005607)**

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

Risk Level: Medium  
CVE: CVE-2014-6322

[Update Details](#)

Risk is updated

**17399 - (MS14-073) Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)**

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

Risk Level: Medium  
CVE: CVE-2014-4116

[Update Details](#)

Risk is updated

**17400 - (MS14-073) Microsoft SharePoint Lists Privilege Escalation (3000431)**

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

Risk Level: Medium  
CVE: CVE-2014-4116

[Update Details](#)

Risk is updated

**17403 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting II (3009712)**

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

Risk Level: Medium  
CVE: CVE-2014-6326

[Update Details](#)

Risk is updated

**17404 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting I (3009712)**

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

Risk Level: Medium  
CVE: CVE-2014-6325

[Update Details](#)

Risk is updated

**17497 - (MS14-080) Microsoft Internet Explorer ASLR Security Bypass (3008923)**

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

Risk Level: Medium  
CVE: CVE-2014-6368

[Update Details](#)

Risk is updated

**17510 - (MS14-080) Microsoft Internet Explorer XSS Filter II Security Bypass (3008923)**

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

Risk Level: Medium

CVE: CVE-2014-6365

[Update Details](#)

Risk is updated

**181297 - FreeBSD unbound Can Be Tricked Into Following An Endless Series Of Delegations, This Consumes A Lot Of Resources (10d73529-7f4b-**

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

Risk Level: Medium

CVE: CVE-2014-8602

[Update Details](#)

Risk is updated

**17402 - (MS14-075) Microsoft Exchange Server OWA URL Redirection Spoofing Information Disclosure (3009712)**

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

Risk Level: Low

CVE: CVE-2014-6336

[Update Details](#)

Risk is updated

**33273 - Oracle Solaris 150817-04 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

**17410 - IBM Tivoli Storage Manager Client ReFS File Unauthorized Access Vulnerability**

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

Risk Level: Low

CVE: CVE-2013-5371

[Update Details](#)

Risk is updated

### 14542 - Mozilla Firefox Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

### 53070 - IBM AIX IP Source Route Receive Status

Category: SSH Module -> NonIntrusive -> AIX Security Policy/Options

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

### 53162 - IBM AIX Other Executable Files Ownership And Permission Settings

Category: SSH Module -> Intrusive -> AIX Security Policy/Options

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

### 70021 - ssl-protocol.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

### 70065 - UnixPolicy.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

## DELETED CHECKS

## 16347 - Microsoft Internet Explorer Flash ActionScript Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-0322

### ADDITIONAL NOTES

- **16347** - has been replaced by FID16406.

### 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 2014 McAfee, Inc.

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