

## MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

### NEW CHECKS

#### 37352 - IBM AIX IV43973 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-5526, CVE-2013-1667

##### Description

The scan detected that the host is missing the following update: IV43973

##### Observation

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

<http://www-01.ibm.com/support/docview.wss?uid=isg1IV43973>

6100-08  
perl.rte < 5.8.8.245

#### 37353 - IBM AIX IV46765 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-5526, CVE-2013-1667

##### Description

The scan detected that the host is missing the following update: IV46765

##### Observation

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

<http://www-01.ibm.com/support/docview.wss?uid=isg1IV46765>

7100-02  
perl.rte < 5.10.1.151

#### 91397 - Oracle Enterprise Linux ELSA-2013-2585 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6545, CVE-2013-0343, CVE-2013-1928, CVE-2013-2164, CVE-2013-2234, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-3231, CVE-2013-4345, CVE-2013-4591

## Description

The scan detected that the host is missing the following update: ELSA-2013-2585

## Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003838.html>

<http://oss.oracle.com/pipermail/el-errata/2013-November/003837.html>

### OEL6

x86\_64

mlnx\_en-2.6.32-400.33.3.el6uekdebug-1.5.7-0.1

ofa-2.6.32-400.33.3.el6uekdebug-1.5.1-4.0.58

kernel-uek-debug-2.6.32-400.33.3.el6uek

kernel-uek-doc-2.6.32-400.33.3.el6uek

kernel-uek-2.6.32-400.33.3.el6uek

kernel-uek-headers-2.6.32-400.33.3.el6uek

kernel-uek-firmware-2.6.32-400.33.3.el6uek

ofa-2.6.32-400.33.3.el6uek-1.5.1-4.0.58

kernel-uek-debug-devel-2.6.32-400.33.3.el6uek

kernel-uek-devel-2.6.32-400.33.3.el6uek

mlnx\_en-2.6.32-400.33.3.el6uek-1.5.7-0.1

i386

mlnx\_en-2.6.32-400.33.3.el6uekdebug-1.5.7-0.1

ofa-2.6.32-400.33.3.el6uekdebug-1.5.1-4.0.58

kernel-uek-debug-2.6.32-400.33.3.el6uek

kernel-uek-doc-2.6.32-400.33.3.el6uek

kernel-uek-2.6.32-400.33.3.el6uek

kernel-uek-headers-2.6.32-400.33.3.el6uek

kernel-uek-firmware-2.6.32-400.33.3.el6uek

ofa-2.6.32-400.33.3.el6uek-1.5.1-4.0.58

kernel-uek-debug-devel-2.6.32-400.33.3.el6uek

kernel-uek-devel-2.6.32-400.33.3.el6uek

mlnx\_en-2.6.32-400.33.3.el6uek-1.5.7-0.1

### OEL5

x86\_64

ofa-2.6.32-400.33.3.el5uekdebug-1.5.1-4.0.58

kernel-uek-headers-2.6.32-400.33.3.el5uek

mlnx\_en-2.6.32-400.33.3.el5uek-1.5.7-2

mlnx\_en-2.6.32-400.33.3.el5uekdebug-1.5.7-2

kernel-uek-devel-2.6.32-400.33.3.el5uek

kernel-uek-firmware-2.6.32-400.33.3.el5uek

kernel-uek-debug-devel-2.6.32-400.33.3.el5uek

ofa-2.6.32-400.33.3.el5uek-1.5.1-4.0.58

kernel-uek-doc-2.6.32-400.33.3.el5uek

kernel-uek-debug-2.6.32-400.33.3.el5uek

kernel-uek-2.6.32-400.33.3.el5uek

i386

ofa-2.6.32-400.33.3.el5uekdebug-1.5.1-4.0.58

kernel-uek-headers-2.6.32-400.33.3.el5uek

mlnx\_en-2.6.32-400.33.3.el5uek-1.5.7-2

mlnx\_en-2.6.32-400.33.3.el5uekdebug-1.5.7-2

kernel-uek-devel-2.6.32-400.33.3.el5uek

kernel-uek-firmware-2.6.32-400.33.3.el5uek

kernel-uek-debug-devel-2.6.32-400.33.3.el5uek  
ofa-2.6.32-400.33.3.el5uek-1.5.1-4.0.58  
kernel-uek-doc-2.6.32-400.33.3.el5uek  
kernel-uek-debug-2.6.32-400.33.3.el5uek  
kernel-uek-2.6.32-400.33.3.el5uek

## 91399 - Oracle Enterprise Linux ELSA-2013-1764 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4164

### Description

The scan detected that the host is missing the following update: ELSA-2013-1764

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003822.html>

### OEL6

#### x86\_64

ruby-libs-1.8.7.352-13.el6  
ruby-static-1.8.7.352-13.el6  
ruby-irb-1.8.7.352-13.el6  
ruby-devel-1.8.7.352-13.el6  
ruby-docs-1.8.7.352-13.el6  
ruby-1.8.7.352-13.el6  
ruby-tcltk-1.8.7.352-13.el6  
ruby-ri-1.8.7.352-13.el6  
ruby-rdoc-1.8.7.352-13.el6

#### i386

ruby-libs-1.8.7.352-13.el6  
ruby-static-1.8.7.352-13.el6  
ruby-irb-1.8.7.352-13.el6  
ruby-devel-1.8.7.352-13.el6  
ruby-docs-1.8.7.352-13.el6  
ruby-1.8.7.352-13.el6  
ruby-tcltk-1.8.7.352-13.el6  
ruby-ri-1.8.7.352-13.el6  
ruby-rdoc-1.8.7.352-13.el6

## 91405 - Oracle Enterprise Linux ELSA-2013-2584 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6545, CVE-2013-0343, CVE-2013-1928, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-3231,  
CVE-2013-4345, CVE-2013-4387, CVE-2013-4592

### Description

The scan detected that the host is missing the following update: ELSA-2013-2584

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003840.html>

<http://oss.oracle.com/pipermail/el-errata/2013-November/003839.html>

#### OEL6

x86\_64

kernel-uek-firmware-2.6.39-400.211.2.el6uek

kernel-uek-doc-2.6.39-400.211.2.el6uek

kernel-uek-debug-2.6.39-400.211.2.el6uek

kernel-uek-debug-devel-2.6.39-400.211.2.el6uek

kernel-uek-devel-2.6.39-400.211.2.el6uek

kernel-uek-2.6.39-400.211.2.el6uek

i386

kernel-uek-firmware-2.6.39-400.211.2.el6uek

kernel-uek-doc-2.6.39-400.211.2.el6uek

kernel-uek-debug-2.6.39-400.211.2.el6uek

kernel-uek-debug-devel-2.6.39-400.211.2.el6uek

kernel-uek-devel-2.6.39-400.211.2.el6uek

kernel-uek-2.6.39-400.211.2.el6uek

#### OEL5

x86\_64

kernel-uek-debug-2.6.39-400.211.2.el5uek

kernel-uek-debug-devel-2.6.39-400.211.2.el5uek

kernel-uek-doc-2.6.39-400.211.2.el5uek

kernel-uek-2.6.39-400.211.2.el5uek

kernel-uek-devel-2.6.39-400.211.2.el5uek

kernel-uek-firmware-2.6.39-400.211.2.el5uek

i386

kernel-uek-debug-2.6.39-400.211.2.el5uek

kernel-uek-debug-devel-2.6.39-400.211.2.el5uek

kernel-uek-doc-2.6.39-400.211.2.el5uek

kernel-uek-2.6.39-400.211.2.el5uek

kernel-uek-devel-2.6.39-400.211.2.el5uek

kernel-uek-firmware-2.6.39-400.211.2.el5uek

## 91406 - Oracle Enterprise Linux ELSA-2013-2583 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0343, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-4345, CVE-2013-4387, CVE-2013-4592

### Description

The scan detected that the host is missing the following update: ELSA-2013-2583

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2013-November/003830.html>

#### OEL6

x86\_64

kernel-uek-firmware-3.8.13-16.2.2.el6uek

dtrace-modules-3.8.13-16.2.2.el6uek-headers-0.4.1-3.el6  
kernel-uek-doc-3.8.13-16.2.2.el6uek  
kernel-uek-debug-3.8.13-16.2.2.el6uek  
kernel-uek-devel-3.8.13-16.2.2.el6uek  
kernel-uek-debug-devel-3.8.13-16.2.2.el6uek  
kernel-uek-3.8.13-16.2.2.el6uek  
dtrace-modules-3.8.13-16.2.2.el6uek-provider-headers-0.4.1-3.el6  
kernel-uek-headers-3.8.13-16.2.2.el6uek  
dtrace-modules-3.8.13-16.2.2.el6uek-0.4.1-3.el6

## 91407 - Oracle Enterprise Linux ELSA-2013-1553 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-6075, CVE-2013-2007, CVE-2013-2231, CVE-2013-4344

### Description

The scan detected that the host is missing the following update: ELSA-2013-1553

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003823.html>

OEL6

x86\_64

qemu-guest-agent-0.12.1.2-2.415.el6

qemu-kvm-tools-0.12.1.2-2.415.el6

qemu-kvm-0.12.1.2-2.415.el6

qemu-img-0.12.1.2-2.415.el6

i386

qemu-guest-agent-0.12.1.2-2.415.el6

## 95882 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 nss-201311-8573 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

### Description

The scan detected that the host is missing the following update: nss-201311-8573

### Observation

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

<http://download.novell.com/Download?buildid=Yj-2lcorlC4~>

<http://download.novell.com/Download?buildid=DBOd7oQkms8~>

<http://download.novell.com/Download?buildid=yIQoxJcWRfg~>

[http://download.novell.com/Download?buildid=xz6litWp\\_m0~](http://download.novell.com/Download?buildid=xz6litWp_m0~)

<http://download.novell.com/Download?buildid=0kIPDxhG3II~>

<http://download.novell.com/Download?buildid=MJyWqjb4z4k~>

<http://download.novell.com/Download?buildid=H-jYbY7v1a0~>

<http://download.novell.com/Download?buildid=ngOJoK7p6P8~>  
<http://download.novell.com/Download?buildid=mMt0mE0MEOo~>

### SuSE SLES 11 SP3

i586

mozilla-nss-tools-3.15.3-0.8.1  
mozilla-nss-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-32bit-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
libsoftokn3-32bit-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-32bit-3.15.3-0.8.1  
mozilla-nss-tools-3.15.3-0.8.1

### SuSE SLED 11

i586

mozilla-nss-tools-3.15.3-0.8.1  
mozilla-nss-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-32bit-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
libsoftokn3-32bit-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-32bit-3.15.3-0.8.1  
mozilla-nss-tools-3.15.3-0.8.1

### SuSE SLED 11 SP3

i586

mozilla-nss-tools-3.15.3-0.8.1  
mozilla-nss-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-32bit-3.15.3-0.8.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.8.1  
libfreebl3-3.15.3-0.8.1  
libsoftokn3-32bit-3.15.3-0.8.1  
libsoftokn3-3.15.3-0.8.1  
libfreebl3-32bit-3.15.3-0.8.1  
mozilla-nss-tools-3.15.3-0.8.1

## SuSE SLES 11

i586

mozilla-nss-tools-3.15.3-0.8.1

mozilla-nss-3.15.3-0.8.1

libsoftokn3-3.15.3-0.8.1

libfreebl3-3.15.3-0.8.1

mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-32bit-3.15.3-0.8.1

mozilla-nspr-4.10.2-0.3.1

mozilla-nspr-32bit-4.10.2-0.3.1

mozilla-nss-3.15.3-0.8.1

libfreebl3-3.15.3-0.8.1

libsoftokn3-32bit-3.15.3-0.8.1

libsoftokn3-3.15.3-0.8.1

libfreebl3-32bit-3.15.3-0.8.1

mozilla-nss-tools-3.15.3-0.8.1

## 95883 - SuSE SLES 10 nss-201311-8758 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

### Description

The scan detected that the host is missing the following update: nss-201311-8758

### Observation

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

For more information see:

<http://download.novell.com/Download?buildid=twluSMVP9PE~>

<http://download.novell.com/Download?buildid=WfNklp8SEW8~>

<http://download.novell.com/Download?buildid=boltZsSQrks~>

## SuSE SLES 10

i586

mozilla-nspr-4.10.2-0.5.1

mozilla-nspr-devel-4.10.2-0.5.1

mozilla-nss-3.15.3-0.5.1

mozilla-nss-devel-3.15.3-0.5.1

mozilla-nss-tools-3.15.3-0.5.1

x86\_64

mozilla-nss-32bit-3.15.3-0.5.1

mozilla-nspr-4.10.2-0.5.1

mozilla-nspr-devel-4.10.2-0.5.1

mozilla-nss-3.15.3-0.5.1

mozilla-nss-devel-3.15.3-0.5.1

mozilla-nss-tools-3.15.3-0.5.1

mozilla-nspr-32bit-4.10.2-0.5.1

## 95884 - SuSE SLED 11 SP2 java-1\_6\_0-openjdk-8598 Update Is Not Installed

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

Risk Level: High

CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5790, CVE-2013-5797, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5820, CVE-2013-5823, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5840, CVE-2013-5842, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851

#### Description

The scan detected that the host is missing the following update: java-1\_6\_0-openjdk-8598

#### Observation

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

[http://download.novell.com/Download?buildid=EKX4O\\_yh2H4~](http://download.novell.com/Download?buildid=EKX4O_yh2H4~)  
<http://download.novell.com/Download?buildid=lb1f3srOpqU~>

SuSE SLED 11 SP2

i586

java-1\_6\_0-openjdk-devel-1.6.0.0\_b27.1.12.7-0.2.1  
java-1\_6\_0-openjdk-1.6.0.0\_b27.1.12.7-0.2.1  
java-1\_6\_0-openjdk-demo-1.6.0.0\_b27.1.12.7-0.2.1

x86\_64

java-1\_6\_0-openjdk-devel-1.6.0.0\_b27.1.12.7-0.2.1  
java-1\_6\_0-openjdk-1.6.0.0\_b27.1.12.7-0.2.1  
java-1\_6\_0-openjdk-demo-1.6.0.0\_b27.1.12.7-0.2.1

### 95886 - SuSE SLES 10 nss-201311-8757 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

#### Description

The scan detected that the host is missing the following update: nss-201311-8757

#### Observation

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

<http://download.novell.com/Download?buildid=ijSMAYNDXdw~>  
<http://download.novell.com/Download?buildid=1SoPNPrtl6l~>  
<http://download.novell.com/Download?buildid=Al7-chCJQOM~>

SuSE SLES 10

i586

mozilla-nspr-4.10.2-0.5.1  
mozilla-nspr-devel-4.10.2-0.5.1  
mozilla-nss-3.15.3-0.5.1  
mozilla-nss-devel-3.15.3-0.5.1  
mozilla-nss-tools-3.15.3-0.5.1

x86\_64

mozilla-nss-32bit-3.15.3-0.5.1  
mozilla-nspr-4.10.2-0.5.1  
mozilla-nspr-devel-4.10.2-0.5.1  
mozilla-nss-3.15.3-0.5.1



mozilla-nss-devel-3.15.3-0.5.1  
mozilla-nss-tools-3.15.3-0.5.1  
mozilla-nspr-32bit-4.10.2-0.5.1

## 95887 - SuSE SLES 11 SP3, SLED 11 SP3 xen-201310-8479 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-1432, CVE-2013-1442, CVE-2013-1918, CVE-2013-4355, CVE-2013-4361, CVE-2013-4368, CVE-2013-4369, CVE-2013-4370, CVE-2013-4371, CVE-2013-4375, CVE-2013-4416

### Description

The scan detected that the host is missing the following update: xen-201310-8479

### Observation

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

<http://download.novell.com/Download?buildid=3ZSjBV2Nck8~>  
<http://download.novell.com/Download?buildid=M22maW8d9y4~>  
<http://download.novell.com/Download?buildid=sv3L0Plu9LU~>  
<http://download.novell.com/Download?buildid=pSpxptnA2IY~>

### SuSE SLES 11 SP3

i586

xen-kmp-default-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-tools-domU-4.2.3\_02-0.7.1  
xen-kmp-pae-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-libs-4.2.3\_02-0.7.1

x86\_64

xen-tools-4.2.3\_02-0.7.1  
xen-libs-32bit-4.2.3\_02-0.7.1  
xen-tools-domU-4.2.3\_02-0.7.1  
xen-4.2.3\_02-0.7.1  
xen-kmp-default-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-libs-4.2.3\_02-0.7.1  
xen-doc-html-4.2.3\_02-0.7.1  
xen-doc-pdf-4.2.3\_02-0.7.1

### SuSE SLED 11 SP3

i586

xen-kmp-default-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-tools-domU-4.2.3\_02-0.7.1  
xen-kmp-pae-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-libs-4.2.3\_02-0.7.1

x86\_64

xen-tools-4.2.3\_02-0.7.1  
xen-libs-32bit-4.2.3\_02-0.7.1  
xen-tools-domU-4.2.3\_02-0.7.1  
xen-4.2.3\_02-0.7.1  
xen-kmp-default-4.2.3\_02\_3.0.93\_0.8-0.7.1  
xen-libs-4.2.3\_02-0.7.1  
xen-doc-html-4.2.3\_02-0.7.1  
xen-doc-pdf-4.2.3\_02-0.7.1

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

Risk Level: High

CVE: CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2013-5607

### Description

The scan detected that the host is missing the following update: nss-201311-8572

### Observation

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

<http://download.novell.com/Download?buildid=saQellYLrol~>  
<http://download.novell.com/Download?buildid=43LCQsvRsfw~>  
<http://download.novell.com/Download?buildid=a82UwfwyVOY~>  
<http://download.novell.com/Download?buildid=V62uKutzco0~>  
<http://download.novell.com/Download?buildid=jESgJkQUr9c~>  
<http://download.novell.com/Download?buildid=5ViAAkeN9Qw~>  
<http://download.novell.com/Download?buildid=3AChQveODZ0~>  
<http://download.novell.com/Download?buildid=fj-Z6mbNN2w~>  
<http://download.novell.com/Download?buildid=CS0TjJfxpN4~>

#### SuSE SLED 11 SP2

i586

mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nss-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
libfreebl3-32bit-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.3.1  
mozilla-nss-32bit-3.15.3-0.3.1

#### SuSE SLED 11

i586

mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nss-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64

mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
libfreebl3-32bit-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.3.1  
mozilla-nss-32bit-3.15.3-0.3.1

#### SuSE SLES 11 SP2

i586

mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nss-3.15.3-0.3.1

libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64  
mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
libfreebl3-32bit-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.3.1  
mozilla-nss-32bit-3.15.3-0.3.1

SuSE SLES 11

i586  
mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nss-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1

x86\_64  
mozilla-nss-tools-3.15.3-0.3.1  
mozilla-nspr-32bit-4.10.2-0.3.1  
libfreebl3-32bit-3.15.3-0.3.1  
libfreebl3-3.15.3-0.3.1  
mozilla-nspr-4.10.2-0.3.1  
mozilla-nss-3.15.3-0.3.1  
mozilla-nss-32bit-3.15.3-0.3.1

## 174391 - Scientific Linux Security ERRATA Critical: ruby on SL6.x i386/x86\_64 (1312-936)

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

Risk Level: High

CVE: CVE-2013-4164

### Description

The scan detected that the host is missing the following update: Security ERRATA Critical: ruby on SL6.x i386/x86\_64 (1312-936)

### Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=936>

SL6

x86\_64  
ruby-libs-1.8.7.352-13.el6  
ruby-static-1.8.7.352-13.el6  
ruby-debuginfo-1.8.7.352-13.el6  
ruby-irb-1.8.7.352-13.el6  
ruby-devel-1.8.7.352-13.el6  
ruby-docs-1.8.7.352-13.el6  
ruby-1.8.7.352-13.el6  
ruby-tcltk-1.8.7.352-13.el6  
ruby-ri-1.8.7.352-13.el6  
ruby-rdoc-1.8.7.352-13.el6

i386

ruby-libs-1.8.7.352-13.el6

ruby-static-1.8.7.352-13.el6  
ruby-debuginfo-1.8.7.352-13.el6  
ruby-irb-1.8.7.352-13.el6  
ruby-devel-1.8.7.352-13.el6  
ruby-docs-1.8.7.352-13.el6  
ruby-1.8.7.352-13.el6  
ruby-tcltk-1.8.7.352-13.el6  
ruby-ri-1.8.7.352-13.el6  
ruby-rdoc-1.8.7.352-13.el6

## 174393 - Scientific Linux Security ERRATA Important: 389-ds-base on SL6.x i386/x86\_64 (1312-318)

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

Risk Level: High

CVE: CVE-2013-4485

### Description

The scan detected that the host is missing the following update: Security ERRATA Important: 389-ds-base on SL6.x i386/x86\_64 (1312-318)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=318>

### SL6

#### x86\_64

p11-kit-devel-0.18.5-2.el6  
openssl-devel-1.0.1e-15.el6  
openssl-perl-1.0.1e-15.el6  
openssl-1.0.1e-15.el6  
389-ds-base-libs-1.2.11.15-30.el6\_5  
p11-kit-trust-0.18.5-2.el6  
389-ds-base-devel-1.2.11.15-30.el6\_5  
p11-kit-0.18.5-2.el6  
389-ds-base-1.2.11.15-30.el6\_5  
389-ds-base-debuginfo-1.2.11.15-30.el6\_5  
openssl-static-1.0.1e-15.el6

### i386

p11-kit-devel-0.18.5-2.el6  
openssl-devel-1.0.1e-15.el6  
openssl-perl-1.0.1e-15.el6  
openssl-1.0.1e-15.el6  
389-ds-base-libs-1.2.11.15-30.el6\_5  
p11-kit-trust-0.18.5-2.el6  
389-ds-base-devel-1.2.11.15-30.el6\_5  
p11-kit-0.18.5-2.el6  
389-ds-base-1.2.11.15-30.el6\_5  
389-ds-base-debuginfo-1.2.11.15-30.el6\_5  
openssl-static-1.0.1e-15.el6

## 177787 - Gentoo Linux GLSA-201311-22 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-5028, CVE-2011-4345, CVE-2011-4711

#### Description

The scan detected that the host is missing the following update: GLSA-201311-22

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-22.xml>

Affected packages:

app-text/namazu < 2.0.21

### 177790 - Gentoo Linux GLSA-201312-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-1168, CVE-2011-2716, CVE-2013-1813

#### Description

The scan detected that the host is missing the following update: GLSA-201312-02

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201312-02.xml>

Affected packages:

sys-apps/busybox < 1.21.0

### 177793 - Gentoo Linux GLSA-201312-04 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-3389

#### Description

The scan detected that the host is missing the following update: GLSA-201312-04

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201312-04.xml>

Affected packages:

media-libs/libtheora < 1.1.1

### 177794 - Gentoo Linux GLSA-201312-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-7250, CVE-2011-1945, CVE-2012-0884, CVE-2012-1165, CVE-2012-2110, CVE-2012-2333, CVE-2012-2686, CVE-2013-0166, CVE-2013-0169

#### Description

The scan detected that the host is missing the following update: GLSA-201312-03

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201312-03.xml>

Affected packages:

dev-libs/openssl < 1.0.0j

dev-libs/openssl < 0.9.8y

### 177795 - Gentoo Linux GLSA-201311-18 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-4528, CVE-2011-4869

#### Description

The scan detected that the host is missing the following update: GLSA-201311-18

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-18.xml>

Affected packages:

net-dns/unbound < 1.4.13\_p2

### 187362 - Fedora Linux 19 FEDORA-2013-21826 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4547

#### Description

The scan detected that the host is missing the following update: FEDORA-2013-21826

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123014.html>

Fedora Core 19

nginx-1.4.4-1.fc19

## 187363 - Fedora Linux 18 FEDORA-2013-21822 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4563

### Description

The scan detected that the host is missing the following update: FEDORA-2013-21822

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122913.html>

Fedora Core 18

kernel-3.11.9-100.fc18

## 15989 - WordPress Platinum SEO Pack Plugin S Parameter Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-5918

### Description

A cross-site scripting vulnerability is present in some versions of the WordPress Platinum SEO Pack plugin.

### Observation

WordPress is a popular blog web application.

A cross-site scripting vulnerability is present in some versions of the WordPress Platinum SEO Pack plugin. The flaw occurs due to improper validation of HTTP requests by the plugin. Successful exploitation could allow an attacker to perform certain administrative actions.

## 15990 - WordPress Social Sharing Toolkit Plugin Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-2701

### Description

A cross-site request forgery vulnerability is present in some versions of the WordPress Social Sharing Toolkit plugin.

### Observation

WordPress is a popular blog web application.

A cross-site request forgery vulnerability is present in some versions of the WordPress Social Sharing Toolkit plugin. The flaw occurs due to improper validation of HTTP requests by the plugin. Successful exploitation could allow an attacker to perform certain administrative actions.

## 85642 - CentOS 5, 6 CESA-2013-1778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-5576, CVE-2013-1913, CVE-2013-1978

### Description

The scan detected that the host is missing the following update: CESA-2013-1778

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-December/020040.html>

<http://lists.centos.org/pipermail/centos-announce/2013-December/020034.html>

#### CentOS 6

i686

gimp-libs-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-devel-tools-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-devel-2.6.9-6.el6\_5

x86\_64

gimp-libs-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-devel-tools-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-devel-2.6.9-6.el6\_5

#### CentOS 5

x86\_64

gimp-libs-2.2.13-3.el5\_10

gimp-devel-2.2.13-3.el5\_10

gimp-2.2.13-3.el5\_10

i386

gimp-libs-2.2.13-3.el5\_10

gimp-devel-2.2.13-3.el5\_10

gimp-2.2.13-3.el5\_10

## 85643 - CentOS 5, 6 CESA-2013-1779 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4566

### Description

The scan detected that the host is missing the following update: CESA-2013-1779

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2013-December/020039.html>



<http://lists.centos.org/pipermail/centos-announce/2013-December/020033.html>

CentOS 6

i686

mod\_nss-1.0.8-19.el6\_5

x86\_64

mod\_nss-1.0.8-19.el6\_5

CentOS 5

x86\_64

mod\_nss-1.0.8-8.el5\_10

i386

mod\_nss-1.0.8-8.el5\_10

### 91401 - Oracle Enterprise Linux ELSA-2013-1536 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2124, CVE-2013-4419

#### Description

The scan detected that the host is missing the following update: ELSA-2013-1536

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2013-November/003825.html>

OEL6

x86\_64:

libguestfs-1.20.11-2.el6.x86\_64.rpm

libguestfs-devel-1.20.11-2.el6.x86\_64.rpm

libguestfs-java-1.20.11-2.el6.x86\_64.rpm

libguestfs-java-devel-1.20.11-2.el6.x86\_64.rpm

libguestfs-javadoc-1.20.11-2.el6.x86\_64.rpm

libguestfs-tools-1.20.11-2.el6.x86\_64.rpm

libguestfs-tools-c-1.20.11-2.el6.x86\_64.rpm

ocaml-libguestfs-1.20.11-2.el6.x86\_64.rpm

ocaml-libguestfs-devel-1.20.11-2.el6.x86\_64.rpm

perl-Sys-Guestfs-1.20.11-2.el6.x86\_64.rpm

python-libguestfs-1.20.11-2.el6.x86\_64.rpm

ruby-libguestfs-1.20.11-2.el6.x86\_64.rpm

### 91402 - Oracle Enterprise Linux ELSA-2013-1582 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4238

#### Description

The scan detected that the host is missing the following update: ELSA-2013-1582

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003819.html>

OEL6

x86\_64

python-libs-2.6.6-51.el6

python-2.6.6-51.el6

python-test-2.6.6-51.el6

tkinter-2.6.6-51.el6

python-tools-2.6.6-51.el6

python-devel-2.6.6-51.el6

i386

python-libs-2.6.6-51.el6

python-2.6.6-51.el6

python-test-2.6.6-51.el6

tkinter-2.6.6-51.el6

python-tools-2.6.6-51.el6

python-devel-2.6.6-51.el6

### 91403 - Oracle Enterprise Linux ELSA-2013-1779 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4566

### Description

The scan detected that the host is missing the following update: ELSA-2013-1779

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-December/003849.html>

OEL6

x86\_64

mod\_nss-1.0.8-19.el6\_5

i386

mod\_nss-1.0.8-19.el6\_5

### 91408 - Oracle Enterprise Linux ELSA-2013-1778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1913, CVE-2013-1978

### Description

The scan detected that the host is missing the following update: ELSA-2013-1778

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-December/003848.html>

OEL6

x86\_64

gimp-libs-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-devel-tools-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-devel-2.6.9-6.el6\_5

i386

gimp-libs-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-devel-tools-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-devel-2.6.9-6.el6\_5

### 95878 - SuSE Linux 12.3 openSUSE-SU-2013:1776-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2925, CVE-2013-2926, CVE-2013-2927, CVE-2013-2928, CVE-2013-2931, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631, CVE-2013-6632

#### Description

The scan detected that the host is missing the following update: openSUSE-SU-2013:1776-1

#### Observation

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

<http://lists.opensuse.org/opensuse-security-announce/2013-11/msg00025.html>

SuSE Linux 12.3

i586

chromium-desktop-kde-31.0.1650.57-1.17.1

chromium-suid-helper-debuginfo-31.0.1650.57-1.17.1

chromium-debugsource-31.0.1650.57-1.17.1

chromium-desktop-gnome-31.0.1650.57-1.17.1

chromium-ffmpegsumo-debuginfo-31.0.1650.57-1.17.1

chromium-debuginfo-31.0.1650.57-1.17.1

chromium-suid-helper-31.0.1650.57-1.17.1

chromium-31.0.1650.57-1.17.1

chromium-ffmpegsumo-31.0.1650.57-1.17.1

chromedriver-debuginfo-31.0.1650.57-1.17.1

chromedriver-31.0.1650.57-1.17.1

### 95879 - SuSE Linux 12.2 openSUSE-SU-2013:1777-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2931, CVE-2013-6621, CVE-2013-6622, CVE-2013-6623, CVE-2013-6624, CVE-2013-6625, CVE-2013-6626, CVE-2013-6627, CVE-2013-6628, CVE-2013-6629, CVE-2013-6630, CVE-2013-6631, CVE-2013-6632

### Description

The scan detected that the host is missing the following update: openSUSE-SU-2013:1777-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-security-announce/2013-11/msg00026.html>

SuSE Linux 12.2

i586

chromium-ffmpegsumo-31.0.1650.57-1.54.1

chromium-desktop-gnome-31.0.1650.57-1.54.1

chromedriver-debuginfo-31.0.1650.57-1.54.1

chromium-suid-helper-debuginfo-31.0.1650.57-1.54.1

chromium-debuginfo-31.0.1650.57-1.54.1

chromium-31.0.1650.57-1.54.1

chromedriver-31.0.1650.57-1.54.1

chromium-desktop-kde-31.0.1650.57-1.54.1

chromium-ffmpegsumo-debuginfo-31.0.1650.57-1.54.1

chromium-debugsource-31.0.1650.57-1.54.1

chromium-suid-helper-31.0.1650.57-1.54.1

## 95885 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 wireshark-8503 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6336, CVE-2013-6337, CVE-2013-6338, CVE-2013-6339, CVE-2013-6340

### Description

The scan detected that the host is missing the following update: wireshark-8503

### Observation

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

For more information see:

<http://download.novell.com/Download?buildid=QmEKN9YgaXQ~>

<http://download.novell.com/Download?buildid=Nlh2e9Ek-6E~>

[http://download.novell.com/Download?buildid=\\_h9\\_IUcbQL4~](http://download.novell.com/Download?buildid=_h9_IUcbQL4~)

<http://download.novell.com/Download?buildid=Fan9gMXtSN8~>

<http://download.novell.com/Download?buildid=355X6oxYEqI~>

<http://download.novell.com/Download?buildid=dq-TLzjdSOU~>

[http://download.novell.com/Download?buildid=c8Sa\\_rfGBfg~](http://download.novell.com/Download?buildid=c8Sa_rfGBfg~)

<http://download.novell.com/Download?buildid=yj-Aq4-ZhZE~>

<http://download.novell.com/Download?buildid=4e145oXI4eU~>

SuSE SLED 11 SP2

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLED 11

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLES 11 SP2

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLES 11

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

## 95888 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 wireshark-8504 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-6336, CVE-2013-6337, CVE-2013-6338, CVE-2013-6339, CVE-2013-6340

### Description

The scan detected that the host is missing the following update: wireshark-8504

### Observation

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

For more information see:

<http://download.novell.com/Download?buildid=mZylEORCdp~>  
<http://download.novell.com/Download?buildid=4T9JHoqR4fQ~>  
<http://download.novell.com/Download?buildid=NjhJtFuVHJk~>  
<http://download.novell.com/Download?buildid=QWioAQs7qw~>  
<http://download.novell.com/Download?buildid=lq7yCOM8Jcs~>  
<http://download.novell.com/Download?buildid=Q7T3OSoaq5E~>  
<http://download.novell.com/Download?buildid=kutEGWas3uQ~>  
<http://download.novell.com/Download?buildid=HSdMFTW5z6s~>  
<http://download.novell.com/Download?buildid=F20SWQeN1U0~>

SuSE SLES 11 SP3

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLED 11

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLED 11 SP3

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

SuSE SLES 11

i586

wireshark-1.8.11-0.2.1

x86\_64

wireshark-1.8.11-0.2.1

## 140363 - Red Hat Enterprise Linux RHSA-2013-1778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-5576, CVE-2013-1913, CVE-2013-1978

### Description

The scan detected that the host is missing the following update: RHSA-2013-1778

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1778.html>

RHEL5D

x86\_64

gimp-debuginfo-2.2.13-3.el5\_10

gimp-libs-2.2.13-3.el5\_10

gimp-2.2.13-3.el5\_10

i386

gimp-debuginfo-2.2.13-3.el5\_10

gimp-libs-2.2.13-3.el5\_10

gimp-2.2.13-3.el5\_10

RHEL6D

x86\_64

gimp-debuginfo-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-libs-2.6.9-6.el6\_5

i386

gimp-debuginfo-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-libs-2.6.9-6.el6\_5

RHEL6WS

x86\_64

gimp-debuginfo-2.6.9-6.el6\_5

gimp-help-browser-2.6.9-6.el6\_5

gimp-2.6.9-6.el6\_5

gimp-libs-2.6.9-6.el6\_5

i386  
gimp-debuginfo-2.6.9-6.el6\_5  
gimp-help-browser-2.6.9-6.el6\_5  
gimp-2.6.9-6.el6\_5  
gimp-libs-2.6.9-6.el6\_5

RHEL5S  
x86\_64  
gimp-debuginfo-2.2.13-3.el5\_10  
gimp-libs-2.2.13-3.el5\_10  
gimp-devel-2.2.13-3.el5\_10  
gimp-2.2.13-3.el5\_10

i386  
gimp-debuginfo-2.2.13-3.el5\_10  
gimp-libs-2.2.13-3.el5\_10  
gimp-devel-2.2.13-3.el5\_10  
gimp-2.2.13-3.el5\_10

RHEL6S  
x86\_64  
gimp-debuginfo-2.6.9-6.el6\_5  
gimp-help-browser-2.6.9-6.el6\_5  
gimp-2.6.9-6.el6\_5  
gimp-libs-2.6.9-6.el6\_5

i386  
gimp-debuginfo-2.6.9-6.el6\_5  
gimp-help-browser-2.6.9-6.el6\_5  
gimp-2.6.9-6.el6\_5  
gimp-libs-2.6.9-6.el6\_5

## 140364 - Red Hat Enterprise Linux RHSA-2013-1779 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4566

### Description

The scan detected that the host is missing the following update: RHSA-2013-1779

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2013-1779.html>

RHEL5D  
x86\_64  
mod\_nss-1.0.8-8.el5\_10  
mod\_nss-debuginfo-1.0.8-8.el5\_10

i386  
mod\_nss-1.0.8-8.el5\_10  
mod\_nss-debuginfo-1.0.8-8.el5\_10

RHEL6D  
x86\_64

mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

i386  
mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

RHEL6WS  
x86\_64  
mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

i386  
mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

RHEL5S  
x86\_64  
mod\_nss-1.0.8-8.el5\_10  
mod\_nss-debuginfo-1.0.8-8.el5\_10

i386  
mod\_nss-1.0.8-8.el5\_10  
mod\_nss-debuginfo-1.0.8-8.el5\_10

RHEL6S  
x86\_64  
mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

i386  
mod\_nss-debuginfo-1.0.8-19.el6\_5  
mod\_nss-1.0.8-19.el6\_5

174392 - Scientific Linux Security ERRATA Moderate: samba4 on SL6.x i386/x86\_64 (1312-1058)

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

Risk Level: Medium

CVE: CVE-2013-4124

#### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: samba4 on SL6.x i386/x86\_64 (1312-1058)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=1058>

SL6  
x86\_64  
samba4-test-4.0.0-58.el6.rc4  
samba4-dc-libs-4.0.0-58.el6.rc4  
samba4-dc-4.0.0-58.el6.rc4  
samba4-devel-4.0.0-58.el6.rc4  
samba4-client-4.0.0-58.el6.rc4  
samba4-pidl-4.0.0-58.el6.rc4



samba4-swat-4.0.0-58.el6.rc4  
samba4-winbind-4.0.0-58.el6.rc4  
samba4-4.0.0-58.el6.rc4  
samba4-debuginfo-4.0.0-58.el6.rc4  
samba4-python-4.0.0-58.el6.rc4  
samba4-libs-4.0.0-58.el6.rc4  
samba4-common-4.0.0-58.el6.rc4  
samba4-winbind-clients-4.0.0-58.el6.rc4  
samba4-winbind-krb5-locator-4.0.0-58.el6.rc4

i386

samba4-test-4.0.0-58.el6.rc4  
samba4-dc-libs-4.0.0-58.el6.rc4  
samba4-dc-4.0.0-58.el6.rc4  
samba4-devel-4.0.0-58.el6.rc4  
samba4-client-4.0.0-58.el6.rc4  
samba4-pidl-4.0.0-58.el6.rc4  
samba4-swat-4.0.0-58.el6.rc4  
samba4-winbind-4.0.0-58.el6.rc4  
samba4-4.0.0-58.el6.rc4  
samba4-debuginfo-4.0.0-58.el6.rc4  
samba4-python-4.0.0-58.el6.rc4  
samba4-libs-4.0.0-58.el6.rc4  
samba4-common-4.0.0-58.el6.rc4  
samba4-winbind-clients-4.0.0-58.el6.rc4  
samba4-winbind-krb5-locator-4.0.0-58.el6.rc4

174395 - Scientific Linux Security ERRATA Moderate: php on SL6.x i386/x86\_64 (1312-814)

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

Risk Level: Medium

CVE: CVE-2006-7243, CVE-2013-1643, CVE-2013-4248

#### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: php on SL6.x i386/x86\_64 (1312-814)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=814>

SL6

x86\_64

php-zts-5.3.3-26.el6  
php-5.3.3-26.el6  
php-pdo-5.3.3-26.el6  
php-debuginfo-5.3.3-26.el6  
php-dba-5.3.3-26.el6  
php-soap-5.3.3-26.el6  
php-devel-5.3.3-26.el6  
php-common-5.3.3-26.el6  
php-ldap-5.3.3-26.el6  
php-cli-5.3.3-26.el6  
php-mbstring-5.3.3-26.el6  
php-bcmath-5.3.3-26.el6  
php-process-5.3.3-26.el6

php-xmlrpc-5.3.3-26.el6  
php-odbc-5.3.3-26.el6  
php-fpm-5.3.3-26.el6  
php-enchant-5.3.3-26.el6  
php-gd-5.3.3-26.el6  
php-pgsql-5.3.3-26.el6  
php-tidy-5.3.3-26.el6  
php-snmp-5.3.3-26.el6  
php-intl-5.3.3-26.el6  
php-xml-5.3.3-26.el6  
php-embedded-5.3.3-26.el6  
php-ispell-5.3.3-26.el6  
php-mysql-5.3.3-26.el6  
php-imap-5.3.3-26.el6  
php-recode-5.3.3-26.el6

i386

php-zts-5.3.3-26.el6  
php-5.3.3-26.el6  
php-pdo-5.3.3-26.el6  
php-debuginfo-5.3.3-26.el6  
php-dba-5.3.3-26.el6  
php-soap-5.3.3-26.el6  
php-devel-5.3.3-26.el6  
php-common-5.3.3-26.el6  
php-ldap-5.3.3-26.el6  
php-cli-5.3.3-26.el6  
php-mbstring-5.3.3-26.el6  
php-bcmath-5.3.3-26.el6  
php-process-5.3.3-26.el6  
php-xmlrpc-5.3.3-26.el6  
php-odbc-5.3.3-26.el6  
php-fpm-5.3.3-26.el6  
php-enchant-5.3.3-26.el6  
php-gd-5.3.3-26.el6  
php-pgsql-5.3.3-26.el6  
php-tidy-5.3.3-26.el6  
php-snmp-5.3.3-26.el6  
php-intl-5.3.3-26.el6  
php-xml-5.3.3-26.el6  
php-embedded-5.3.3-26.el6  
php-ispell-5.3.3-26.el6  
php-mysql-5.3.3-26.el6  
php-imap-5.3.3-26.el6  
php-recode-5.3.3-26.el6

## 174396 - Scientific Linux Security ERRATA Moderate: libguestfs on SL6.x x86\_64 (1312-196)

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

Risk Level: Medium

CVE: CVE-2013-4419

### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: libguestfs on SL6.x x86\_64 (1312-196)

### Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=196>

SL6

x86\_64

febootstrap-supermin-helper-3.21-4.el6

ruby-libguestfs-1.20.11-2.el6

libguestfs-1.20.11-2.el6

febootstrap-3.21-4.el6

ocaml-libguestfs-1.20.11-2.el6

perl-Sys-Guestfs-1.20.11-2.el6

libguestfs-devel-1.20.11-2.el6

libguestfs-java-1.20.11-2.el6

ocaml-libguestfs-devel-1.20.11-2.el6

python-libguestfs-1.20.11-2.el6

libguestfs-tools-1.20.11-2.el6

libguestfs-tools-c-1.20.11-2.el6

libguestfs-javadoc-1.20.11-2.el6

libguestfs-java-devel-1.20.11-2.el6

libguestfs-debuginfo-1.20.11-2.el6

174397 - Scientific Linux Security ERRATA Moderate: glibc on SL6.x i386/x86\_64 (1312-448)

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

Risk Level: Medium

CVE: CVE-2013-0242, CVE-2013-1914, CVE-2013-4332

#### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: glibc on SL6.x i386/x86\_64 (1312-448)

#### Observation

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

For more information see:

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=448>

SL6

x86\_64

glibc-utils-2.12-1.132.el6

glibc-headers-2.12-1.132.el6

glibc-2.12-1.132.el6

glibc-static-2.12-1.132.el6

glibc-devel-2.12-1.132.el6

nscd-2.12-1.132.el6

glibc-common-2.12-1.132.el6

glibc-debuginfo-2.12-1.132.el6

glibc-debuginfo-common-2.12-1.132.el6

i386

glibc-utils-2.12-1.132.el6

glibc-headers-2.12-1.132.el6

glibc-2.12-1.132.el6

glibc-static-2.12-1.132.el6

glibc-devel-2.12-1.132.el6

nscd-2.12-1.132.el6

glibc-common-2.12-1.132.el6

glibc-debuginfo-2.12-1.132.el6  
glibc-debuginfo-common-2.12-1.132.el6

#### 174399 - Scientific Linux Security ERRATA Moderate: python on SL6.x i386/x86\_64 (1312-1182)

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

Risk Level: Medium

CVE: CVE-2013-4238

##### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: python on SL6.x i386/x86\_64 (1312-1182)

##### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=1182>

SL6  
x86\_64  
python-debuginfo-2.6.6-51.el6  
python-2.6.6-51.el6  
python-test-2.6.6-51.el6  
tkinter-2.6.6-51.el6  
python-tools-2.6.6-51.el6  
python-libs-2.6.6-51.el6  
python-devel-2.6.6-51.el6

i386  
python-debuginfo-2.6.6-51.el6  
python-2.6.6-51.el6  
python-test-2.6.6-51.el6  
tkinter-2.6.6-51.el6  
python-tools-2.6.6-51.el6  
python-libs-2.6.6-51.el6  
python-devel-2.6.6-51.el6

#### 174400 - Scientific Linux Security ERRATA Moderate: luci on SL6.x i386/x86\_64 (1312-1429)

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

Risk Level: Medium

CVE: CVE-2013-4481, CVE-2013-4482

##### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: luci on SL6.x i386/x86\_64 (1312-1429)

##### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=1429>

SL6

x86\_64  
luci-0.26.0-48.el6  
luci-debuginfo-0.26.0-48.el6

i386  
luci-0.26.0-48.el6  
luci-debuginfo-0.26.0-48.el6

## 174401 - Scientific Linux Security ERRATA Moderate: samba on SL6.x i386/x86\_64 (1312-1306)

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

Risk Level: Medium

CVE: CVE-2013-0213, CVE-2013-0214, CVE-2013-4124

### Description

The scan detected that the host is missing the following update: Security ERRATA Moderate: samba on SL6.x i386/x86\_64 (1312-1306)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=1306>

### SL6

x86\_64  
libsmbclient-3.6.9-164.el6  
libtevent-0.9.18-3.el6  
libtevent-devel-0.9.18-3.el6  
samba-client-3.6.9-164.el6  
samba-3.6.9-164.el6  
samba-winbind-devel-3.6.9-164.el6  
libsmbclient-devel-3.6.9-164.el6  
samba-common-3.6.9-164.el6  
samba-doc-3.6.9-164.el6  
samba-winbind-clients-3.6.9-164.el6  
samba-debuginfo-3.6.9-164.el6  
samba-winbind-krb5-locator-3.6.9-164.el6  
samba-winbind-3.6.9-164.el6  
samba-swat-3.6.9-164.el6  
samba-domainjoin-gui-3.6.9-164.el6

### i386

libsmbclient-3.6.9-164.el6  
libtevent-0.9.18-3.el6  
libtevent-devel-0.9.18-3.el6  
samba-client-3.6.9-164.el6  
samba-3.6.9-164.el6  
samba-winbind-devel-3.6.9-164.el6  
libsmbclient-devel-3.6.9-164.el6  
samba-common-3.6.9-164.el6  
samba-doc-3.6.9-164.el6  
samba-winbind-clients-3.6.9-164.el6  
samba-debuginfo-3.6.9-164.el6  
samba-winbind-krb5-locator-3.6.9-164.el6  
samba-winbind-3.6.9-164.el6  
samba-swat-3.6.9-164.el6  
samba-domainjoin-gui-3.6.9-164.el6

## 177786 - Gentoo Linux GLSA-201311-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-2575

### Description

The scan detected that the host is missing the following update: GLSA-201311-20

### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-20.xml>

Affected packages:

kde-base/okular < 4.4.5-r2

## 177788 - Gentoo Linux GLSA-201311-17 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2008-5302, CVE-2008-5303, CVE-2010-1158, CVE-2011-0761, CVE-2011-1487

### Description

The scan detected that the host is missing the following update: GLSA-201311-17

### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-17.xml>

Affected packages:

dev-lang/perl < 5.12.3-r1

## 177789 - Gentoo Linux GLSA-201311-21 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-0624

### Description

The scan detected that the host is missing the following update: GLSA-201311-21

### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-21.xml>

Affected packages:

app-arch/cpio < 2.11

### 177791 - Gentoo Linux GLSA-201311-19 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2252, CVE-2012-3478

#### Description

The scan detected that the host is missing the following update: GLSA-201311-19

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201311-19.xml>

Affected packages:

app-shells/rssh < 2.3.4

### 177792 - Gentoo Linux GLSA-201312-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-5029, CVE-2010-3847, CVE-2011-0536, CVE-2011-1071, CVE-2011-1089, CVE-2011-1095, CVE-2011-1658, CVE-2011-1659, CVE-2012-0864

#### Description

The scan detected that the host is missing the following update: GLSA-201312-01

#### Observation

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

<http://security.gentoo.org/glsa/glsa-201312-01.xml>

Affected packages:

sys-libs/glibc < 2.15-r3

### 184223 - Ubuntu Linux 13.04 USN-2046-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4470

#### Description

The scan detected that the host is missing the following update: USN-2046-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002334.html>

Ubuntu 13.04

linux-image-3.5.0-236-omap4\_3.5.0-236.52

### 184224 - Ubuntu Linux 12.10 USN-2043-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4470

#### Description

The scan detected that the host is missing the following update: USN-2043-1

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002331.html>

Ubuntu 12.10

linux-image-3.5.0-44-powerpc64-smp\_3.5.0-44.67

linux-image-3.5.0-44-omap\_3.5.0-44.67

linux-image-3.5.0-44-powerpc-smp\_3.5.0-44.67

linux-image-3.5.0-44-generic\_3.5.0-44.67

linux-image-3.5.0-44-highbank\_3.5.0-44.67

### 184225 - Ubuntu Linux 10.04 USN-2036-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2121, CVE-2013-4511

#### Description

The scan detected that the host is missing the following update: USN-2036-1

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002324.html>

Ubuntu 10.04

linux-image-2.6.32-54-generic-pae\_2.6.32-54.116

linux-image-2.6.32-54-lpia\_2.6.32-54.116

linux-image-2.6.32-54-versatile\_2.6.32-54.116

linux-image-2.6.32-54-preempt\_2.6.32-54.116

linux-image-2.6.32-54-server\_2.6.32-54.116

linux-image-2.6.32-54-powerpc\_2.6.32-54.116

linux-image-2.6.32-54-386\_2.6.32-54.116

linux-image-2.6.32-54-sparc64-smp\_2.6.32-54.116

linux-image-2.6.32-54-powerpc64-smp\_2.6.32-54.116

linux-image-2.6.32-54-sparc64\_2.6.32-54.116



linux-image-2.6.32-54-ia64\_2.6.32-54.116  
linux-image-2.6.32-54-powerpc-smp\_2.6.32-54.116  
linux-image-2.6.32-54-generic\_2.6.32-54.116  
linux-image-2.6.32-54-virtual\_2.6.32-54.116

#### 184226 - Ubuntu Linux 12.04 USN-2040-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4470

##### Description

The scan detected that the host is missing the following update: USN-2040-1

##### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002328.html>

Ubuntu 12.04

linux-image-3.5.0-44-generic\_3.5.0-44.67~precise1

#### 184227 - Ubuntu Linux 12.10 USN-2044-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4470

##### Description

The scan detected that the host is missing the following update: USN-2044-1

##### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002332.html>

Ubuntu 12.10

linux-image-3.5.0-236-omap4\_3.5.0-236.52

#### 184228 - Ubuntu Linux 13.04 USN-2045-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4350, CVE-2013-4387

##### Description

The scan detected that the host is missing the following update: USN-2045-1

##### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002333.html>

Ubuntu 13.04

linux-image-3.8.0-34-generic\_3.8.0-34.49

#### 184230 - Ubuntu Linux 12.04 USN-2041-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4350, CVE-2013-4387

##### Description

The scan detected that the host is missing the following update: USN-2041-1

##### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002329.html>

Ubuntu 12.04

linux-image-3.8.0-34-generic\_3.8.0-34.49~precise1

#### 184231 - Ubuntu Linux 10.04 USN-2037-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2121, CVE-2013-4511

##### Description

The scan detected that the host is missing the following update: USN-2037-1

##### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002325.html>

Ubuntu 10.04

linux-image-2.6.32-359-ec2\_2.6.32-359.72

#### 184232 - Ubuntu Linux 12.04 USN-2042-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4299, CVE-2013-4470

##### Description

The scan detected that the host is missing the following update: USN-2042-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002330.html>

Ubuntu 12.04

linux-image-3.11.0-14-generic-lpae\_3.11.0-14.21~precise1

linux-image-3.11.0-14-generic\_3.11.0-14.21~precise1

#### 184233 - Ubuntu Linux 12.04 USN-2039-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0343, CVE-2013-2140, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-2893, CVE-2013-2895, CVE-2013-2896, CVE-2013-2897, CVE-2013-2899, CVE-2013-4350, CVE-2013-4387

#### Description

The scan detected that the host is missing the following update: USN-2039-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002327.html>

Ubuntu 12.04

linux-image-3.2.0-1441-omap4\_3.2.0-1441.60

#### 184234 - Ubuntu Linux 12.04 USN-2038-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-0343, CVE-2013-2140, CVE-2013-2888, CVE-2013-2889, CVE-2013-2892, CVE-2013-2893, CVE-2013-2895, CVE-2013-2896, CVE-2013-2897, CVE-2013-2899, CVE-2013-4350, CVE-2013-4387

#### Description

The scan detected that the host is missing the following update: USN-2038-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002326.html>

Ubuntu 12.04

linux-image-3.2.0-57-virtual\_3.2.0-57.87

linux-image-3.2.0-57-generic\_3.2.0-57.87

linux-image-3.2.0-57-powerpc-smp\_3.2.0-57.87

linux-image-3.2.0-57-highbank\_3.2.0-57.87  
linux-image-3.2.0-57-generic-pae\_3.2.0-57.87  
linux-image-3.2.0-57-omap\_3.2.0-57.87  
linux-image-3.2.0-57-powerpc64-smp\_3.2.0-57.87

## 184235 - Ubuntu Linux 12.04, 12.10, 13.04, 13.10 USN-2035-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2065, CVE-2013-4164

### Description

The scan detected that the host is missing the following update: USN-2035-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-November/002323.html>

#### Ubuntu 12.10

libruby1.8\_1.8.7.358-4ubuntu0.4  
ruby1.8\_1.8.7.358-4ubuntu0.4  
libruby1.9.1\_1.9.3.194-1ubuntu1.6  
ruby1.9.1\_1.9.3.194-1ubuntu1.6

#### Ubuntu 13.10

ruby1.9.1\_1.9.3.194-8.1ubuntu2.1  
libruby1.8\_1.8.7.358-7ubuntu2.1  
libruby1.9.1\_1.9.3.194-8.1ubuntu2.1  
ruby1.8\_1.8.7.358-7ubuntu2.1

#### Ubuntu 12.04

ruby1.8\_1.8.7.352-2ubuntu1.4  
ruby1.9.1\_1.9.3.0-1ubuntu2.8  
libruby1.8\_1.8.7.352-2ubuntu1.4  
libruby1.9.1\_1.9.3.0-1ubuntu2.8

#### Ubuntu 13.04

libruby1.9.1\_1.9.3.194-8.1ubuntu1.2  
ruby1.9.1\_1.9.3.194-8.1ubuntu1.2  
ruby1.8\_1.8.7.358-7ubuntu1.2  
libruby1.8\_1.8.7.358-7ubuntu1.2

## 187358 - Fedora Linux 19 FEDORA-2013-22012 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4485

### Description

The scan detected that the host is missing the following update: FEDORA-2013-22012

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123036.html>

Fedora Core 19

389-ds-base-1.3.1.16-1.fc19

### 187360 - Fedora Linux 19 FEDORA-2013-21887 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4545

### Description

The scan detected that the host is missing the following update: FEDORA-2013-21887

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123009.html>

Fedora Core 19

mingw-curl-7.33.0-1.fc19

### 187364 - Fedora Linux 19 FEDORA-2013-21786 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-1417, CVE-2013-1418

### Description

The scan detected that the host is missing the following update: FEDORA-2013-21786

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123064.html>

Fedora Core 19

krb5-1.11.3-13.fc19

### 58734 - Debian Linux 6.0, 7.0 DSA-2805-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4478, CVE-2013-4479

### Description

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

### Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00219.html>

Debian 7.0

all  
sup-mail\_0.12.1+git20120407.aaa852f-1+deb7u1

Debian 6.0

all  
sup-mail\_0.11-2+nmu1+deb6u1

## 58735 - Debian Linux 6.0, 7.0 DSA-2806-1 Update Is Not Installed

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

Risk Level: Low

### Description

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

### Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00220.html>

Debian 7.0

i386  
nbd-server\_3.2-4~deb7u4  
nbd-client\_3.2-4~deb7u4

Debian 6.0

i386  
nbd-server\_2.9.16-8+squeeze1  
nbd-client\_2.9.16-8+squeeze1

## 58736 - Debian Linux 6.0, 7.0 DSA-2808-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1447, CVE-2013-6045, CVE-2013-6052, CVE-2013-6054

### Description

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

### Observation

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

<http://lists.debian.org/debian-security-announce/2013/msg00222.html>

Debian 7.0

i386

libopenjpeg-dev\_1.3+dfsg-4.7

libopenjpeg2-dbg\_1.3+dfsg-4.7

openjpeg-tools\_1.3+dfsg-4.7

libopenjpeg2\_1.3+dfsg-4.7

Debian 6.0

i386

libopenjpeg-dev\_1.3+dfsg-4+squeeze2

openjpeg-tools\_1.3+dfsg-4+squeeze2

libopenjpeg2-dbg\_1.3+dfsg-4+squeeze2

libopenjpeg2\_1.3+dfsg-4+squeeze2

### 58737 - Debian Linux 6.0, 7.0 DSA-2807-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6050

#### Description

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

#### Observation

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

For more information see:

<http://lists.debian.org/debian-security-announce/2013/msg00221.html>

Debian 7.0

i386

links2\_2.7-1+deb7u1

links\_2.7-1+deb7u1

Debian 6.0

i386

links\_2.3~pre1-1+squeeze2

links2\_2.3~pre1-1+squeeze2

### 91398 - Oracle Enterprise Linux ELSA-2013-1620 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-1940, CVE-2013-4396

#### Description

The scan detected that the host is missing the following update: ELSA-2013-1620

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2013-November/003821.html>

OEL6

x86\_64

xorg-x11-server-Xvfb-1.13.0-23.el6  
xorg-x11-server-common-1.13.0-23.el6  
xorg-x11-server-source-1.13.0-23.el6  
xorg-x11-server-Xorg-1.13.0-23.el6  
xorg-x11-server-Xnest-1.13.0-23.el6  
xorg-x11-server-Xdmx-1.13.0-23.el6  
xorg-x11-server-devel-1.13.0-23.el6  
xorg-x11-server-Xephyr-1.13.0-23.el6

i386

xorg-x11-server-Xvfb-1.13.0-23.el6  
xorg-x11-server-common-1.13.0-23.el6  
xorg-x11-server-source-1.13.0-23.el6  
xorg-x11-server-Xorg-1.13.0-23.el6  
xorg-x11-server-Xnest-1.13.0-23.el6  
xorg-x11-server-Xdmx-1.13.0-23.el6  
xorg-x11-server-devel-1.13.0-23.el6  
xorg-x11-server-Xephyr-1.13.0-23.el6

## 91400 - Oracle Enterprise Linux ELSA-2013-1591 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2010-5107

### Description

The scan detected that the host is missing the following update: ELSA-2013-1591

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2013-November/003820.html>

OEL6

x86\_64

pam\_ssh\_agent\_auth-0.9.3-94.el6  
openssh-server-5.3p1-94.el6  
openssh-askpass-5.3p1-94.el6  
openssh-ldap-5.3p1-94.el6  
openssh-5.3p1-94.el6  
openssh-clients-5.3p1-94.el6

i386

pam\_ssh\_agent\_auth-0.9.3-94.el6  
openssh-server-5.3p1-94.el6  
openssh-askpass-5.3p1-94.el6  
openssh-ldap-5.3p1-94.el6  
openssh-5.3p1-94.el6  
openssh-clients-5.3p1-94.el6

## 91404 - Oracle Enterprise Linux ELSA-2013-1540 Update Is Not Installed



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

Risk Level: Low

CVE: CVE-2013-4166

### Description

The scan detected that the host is missing the following update: ELSA-2013-1540

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2013-November/003824.html>

OEL6

x86\_64

control-center-devel-2.28.1-39.el6

cheese-2.28.1-8.el6

control-center-2.28.1-39.el6

finch-2.7.9-11.el6

evolution-spamassassin-2.32.3-30.el6

totem-upnp-2.28.6-4.el6

evolution-devel-docs-2.32.3-30.el6

evolution-perl-2.32.3-30.el6

openchange-devel-1.0-6.el6

gnome-python2-metacity-2.28.0-5.el6

gnome-python2-totem-2.28.0-5.el6

evolution-data-server-doc-2.32.3-18.el6

gnome-panel-devel-2.30.2-15.el6

control-center-filesystem-2.28.1-39.el6

gtkhtml3-devel-3.32.2-2.el6

planner-devel-0.14.4-10.el6

evolution-2.32.3-30.el6

gnome-python2-desktop-2.28.0-5.el6

libpurple-perl-2.7.9-11.el6

libgdata-0.6.4-2.el6

gnome-python2-gnomeprint-2.28.0-5.el6

gnome-python2-bugbuddy-2.28.0-5.el6

evolution-pst-2.32.3-30.el6

totem-youtube-2.28.6-4.el6

gnome-python2-evinced-2.28.0-5.el6

gnome-python2-applet-2.28.0-5.el6

totem-nautilus-2.28.6-4.el6

gnome-panel-2.30.2-15.el6

evolution-exchange-2.32.3-16.el6

gnome-python2-gnomekeyring-2.28.0-5.el6

evolution-devel-2.32.3-30.el6

gnome-python2-gtksourceview-2.28.0-5.el6

libpurple-2.7.9-11.el6

totem-jamendo-2.28.6-4.el6

evolution-mapi-0.32.2-12.el6

pidgin-devel-2.7.9-11.el6

libgdata-devel-0.6.4-2.el6

pidgin-2.7.9-11.el6

gnome-python2-evolution-2.28.0-5.el6

openchange-devel-docs-1.0-6.el6

gnome-python2-libwnck-2.28.0-5.el6

openchange-client-1.0-6.el6

totem-devel-2.28.6-4.el6

totem-mozplugin-2.28.6-4.el6  
nautilus-sendto-devel-2.28.2-4.el6  
gnome-python2-libgtop2-2.28.0-5.el6  
openchange-1.0-6.el6  
pidgin-perl-2.7.9-11.el6  
planner-0.14.4-10.el6  
libpurple-devel-2.7.9-11.el6  
control-center-extra-2.28.1-39.el6  
totem-2.28.6-4.el6  
gnome-python2-gnomedesktop-2.28.0-5.el6  
evolution-mapi-devel-0.32.2-12.el6  
gnome-panel-libs-2.30.2-15.el6  
finch-devel-2.7.9-11.el6  
planner-eds-0.14.4-10.el6  
nautilus-sendto-2.28.2-4.el6  
ekiga-3.2.6-4.el6  
libpurple-tcl-2.7.9-11.el6  
gnome-python2-brasero-2.28.0-5.el6  
gnome-python2-rsvg-2.28.0-5.el6  
evolution-help-2.32.3-30.el6  
gtkhtml3-3.32.2-2.el6  
evolution-data-server-devel-2.32.3-18.el6  
pidgin-docs-2.7.9-11.el6  
evolution-data-server-2.32.3-18.el6

i386

control-center-devel-2.28.1-39.el6  
cheese-2.28.1-8.el6  
control-center-2.28.1-39.el6  
finch-2.7.9-11.el6  
evolution-spamassassin-2.32.3-30.el6  
totem-upnp-2.28.6-4.el6  
evolution-devel-docs-2.32.3-30.el6  
evolution-perl-2.32.3-30.el6  
openchange-devel-1.0-6.el6  
gnome-python2-metacity-2.28.0-5.el6  
gnome-python2-totem-2.28.0-5.el6  
evolution-data-server-doc-2.32.3-18.el6  
gnome-panel-devel-2.30.2-15.el6  
control-center-filesystem-2.28.1-39.el6  
gtkhtml3-devel-3.32.2-2.el6  
planner-devel-0.14.4-10.el6  
evolution-2.32.3-30.el6  
gnome-python2-desktop-2.28.0-5.el6  
libpurple-perl-2.7.9-11.el6  
libgdata-0.6.4-2.el6  
gnome-python2-gnomeprint-2.28.0-5.el6  
gnome-python2-bugbuddy-2.28.0-5.el6  
evolution-pst-2.32.3-30.el6  
totem-youtube-2.28.6-4.el6  
gnome-python2-evinced-2.28.0-5.el6  
gnome-python2-applet-2.28.0-5.el6  
totem-nautilus-2.28.6-4.el6  
gnome-panel-2.30.2-15.el6  
evolution-exchange-2.32.3-16.el6  
gnome-python2-gnomekeyring-2.28.0-5.el6  
evolution-devel-2.32.3-30.el6  
gnome-python2-gtksourceview-2.28.0-5.el6  
libpurple-2.7.9-11.el6  
totem-jamendo-2.28.6-4.el6

evolution-mapi-0.32.2-12.el6  
pidgin-devel-2.7.9-11.el6  
libgdata-devel-0.6.4-2.el6  
pidgin-2.7.9-11.el6  
gnome-python2-evolution-2.28.0-5.el6  
openchange-devel-docs-1.0-6.el6  
gnome-python2-libwnck-2.28.0-5.el6  
openchange-client-1.0-6.el6  
totem-devel-2.28.6-4.el6  
totem-mozplugin-2.28.6-4.el6  
nautilus-sendto-devel-2.28.2-4.el6  
gnome-python2-libgtop2-2.28.0-5.el6  
openchange-1.0-6.el6  
pidgin-perl-2.7.9-11.el6  
planner-0.14.4-10.el6  
libpurple-devel-2.7.9-11.el6  
control-center-extra-2.28.1-39.el6  
totem-2.28.6-4.el6  
gnome-python2-gnomedesktop-2.28.0-5.el6  
evolution-mapi-devel-0.32.2-12.el6  
gnome-panel-libs-2.30.2-15.el6  
finch-devel-2.7.9-11.el6  
planner-eds-0.14.4-10.el6  
nautilus-sendto-2.28.2-4.el6  
ekiga-3.2.6-4.el6  
libpurple-tcl-2.7.9-11.el6  
gnome-python2-brasero-2.28.0-5.el6  
gnome-python2-rsvg-2.28.0-5.el6  
evolution-help-2.32.3-30.el6  
gtkhtml3-3.32.2-2.el6  
evolution-data-server-devel-2.32.3-18.el6  
pidgin-docs-2.7.9-11.el6  
evolution-data-server-2.32.3-18.el6

## 95880 - SuSE SLES 11, 11 SP2, SLED 11, 11 SP2 openvpn-8496 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2061

### Description

The scan detected that the host is missing the following update: openvpn-8496

### Observation

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

<http://download.novell.com/Download?buildid=Dt-H24ARLk~>  
<http://download.novell.com/Download?buildid=GVVOzQgm~>  
<http://download.novell.com/Download?buildid=D10oDH4nYr~>  
<http://download.novell.com/Download?buildid=XcdmhKZtFv0~>  
<http://download.novell.com/Download?buildid=aR3hrI2RErU~>  
<http://download.novell.com/Download?buildid=Y28arLgAOMM~>  
<http://download.novell.com/Download?buildid=ImaAWXVtZNs~>  
<http://download.novell.com/Download?buildid=JHP9V5XgVc8~>  
<http://download.novell.com/Download?buildid=RLqUhtT4aJw~>

SuSE SLED 11 SP2

i586  
openvpn-2.0.9-143.33.3.1

x86\_64  
openvpn-2.0.9-143.33.3.1

SuSE SLED 11  
i586  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

x86\_64  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

SuSE SLES 11 SP2  
i586  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

x86\_64  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

SuSE SLES 11  
i586  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

x86\_64  
openvpn-2.0.9-143.33.3.1  
openvpn-auth-pam-plugin-2.0.9-143.33.3.1

## 95881 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 openvpn-8493 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-2061

### Description

The scan detected that the host is missing the following update: openvpn-8493

### Observation

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

<http://download.novell.com/Download?buildid=tis-zROdirU~>  
<http://download.novell.com/Download?buildid=i1cupVkJBmk~>  
[http://download.novell.com/Download?buildid=rIgBdu\\_Sk4E~](http://download.novell.com/Download?buildid=rIgBdu_Sk4E~)  
<http://download.novell.com/Download?buildid=Fztyp7Fnu2Q~>  
<http://download.novell.com/Download?buildid=7OnCxmXj3RA~>  
<http://download.novell.com/Download?buildid=HIOuo1sXM0k~>  
<http://download.novell.com/Download?buildid=cWE1wZiT1nl~>  
<http://download.novell.com/Download?buildid=PZNGXJpUFvc~>  
<http://download.novell.com/Download?buildid=t0suAbHefWU~>

SuSE SLES 11 SP3  
i586

openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

x86\_64  
openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

SuSE SLED 11  
i586  
openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

x86\_64  
openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

SuSE SLED 11 SP3  
i586  
openvpn-2.0.9-143.40.5

x86\_64  
openvpn-2.0.9-143.40.5

SuSE SLES 11  
i586  
openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

x86\_64  
openvpn-auth-pam-plugin-2.0.9-143.40.5  
openvpn-2.0.9-143.40.5

## 174390 - Scientific Linux Security ERRATA Low: openssh on SL6.x i386/x86\_64 (1312-571)

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

Risk Level: Low

CVE: CVE-2010-5107

### Description

The scan detected that the host is missing the following update: Security ERRATA Low: openssh on SL6.x i386/x86\_64 (1312-571)

### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=571>

SL6  
x86\_64  
openssl-devel-1.0.1e-15.el6  
pam\_ssh\_agent\_auth-0.9.3-94.el6  
openssl-perl-1.0.1e-15.el6  
openssl-1.0.1e-15.el6  
openssh-server-5.3p1-94.el6  
openssh-debuginfo-5.3p1-94.el6  
openssh-askpass-5.3p1-94.el6  
openssh-ldap-5.3p1-94.el6

openssh-5.3p1-94.el6  
openssh-clients-5.3p1-94.el6  
openssl-static-1.0.1e-15.el6

i386

openssl-devel-1.0.1e-15.el6  
pam\_ssh\_agent\_auth-0.9.3-94.el6  
openssl-perl-1.0.1e-15.el6  
openssl-1.0.1e-15.el6  
openssh-server-5.3p1-94.el6  
openssh-debuginfo-5.3p1-94.el6  
openssh-askpass-5.3p1-94.el6  
openssh-ldap-5.3p1-94.el6  
openssh-5.3p1-94.el6  
openssh-clients-5.3p1-94.el6  
openssl-static-1.0.1e-15.el6

174394 - Scientific Linux Security ERRATA Low: pacemaker on SL6.x i386/x86\_64 (1312-691)

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

Risk Level: Low

CVE: CVE-2013-0281

#### Description

The scan detected that the host is missing the following update: Security ERRATA Low: pacemaker on SL6.x i386/x86\_64 (1312-691)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=691>

SL6

x86\_64

fence-agents-3.1.5-35.el6  
corosync-1.4.1-17.el6  
libqb-0.16.0-2.el6  
corosynclib-devel-1.4.1-17.el6  
pacemaker-debuginfo-1.1.10-14.el6  
pacemaker-doc-1.1.10-14.el6  
luci-0.26.0-48.el6  
pacemaker-cluster-libs-1.1.10-14.el6  
pacemaker-cli-1.1.10-14.el6  
pacemaker-1.1.10-14.el6  
clusterlib-devel-3.0.12.1-59.el6  
pacemaker-remote-1.1.10-14.el6  
pacemaker-cts-1.1.10-14.el6  
gfs2-utils-3.0.12.1-59.el6  
pacemaker-libs-1.1.10-14.el6  
cman-3.0.12.1-59.el6  
corosynclib-1.4.1-17.el6  
pacemaker-libs-devel-1.1.10-14.el6  
libqb-devel-0.16.0-2.el6  
clusterlib-3.0.12.1-59.el6

i386

fence-agents-3.1.5-35.el6

corosync-1.4.1-17.el6  
libqb-0.16.0-2.el6  
corosynclib-devel-1.4.1-17.el6  
pacemaker-debuginfo-1.1.10-14.el6  
pacemaker-doc-1.1.10-14.el6  
luci-0.26.0-48.el6  
pacemaker-cluster-libs-1.1.10-14.el6  
pacemaker-cli-1.1.10-14.el6  
pacemaker-1.1.10-14.el6  
clusterlib-devel-3.0.12.1-59.el6  
pacemaker-remote-1.1.10-14.el6  
pacemaker-cts-1.1.10-14.el6  
gfs2-utils-3.0.12.1-59.el6  
pacemaker-libs-1.1.10-14.el6  
cman-3.0.12.1-59.el6  
corosynclib-1.4.1-17.el6  
pacemaker-libs-devel-1.1.10-14.el6  
libqb-devel-0.16.0-2.el6  
clusterlib-3.0.12.1-59.el6

#### 174398 - Scientific Linux Security ERRATA Low: augeas on SL6.x i386/x86\_64 (1312-79)

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

Risk Level: Low

CVE: CVE-2012-0786, CVE-2012-0787

#### Description

The scan detected that the host is missing the following update: Security ERRATA Low: augeas on SL6.x i386/x86\_64 (1312-79)

#### Observation

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

<http://listserv.fnal.gov/scripts/wa.exe?A2=ind1312&L=scientific-linux-errata&T=0&P=79>

#### SL6

##### x86\_64

augeas-libs-1.0.0-5.el6  
augeas-debuginfo-1.0.0-5.el6  
augeas-1.0.0-5.el6  
augeas-devel-1.0.0-5.el6

##### i386

augeas-libs-1.0.0-5.el6  
augeas-debuginfo-1.0.0-5.el6  
augeas-1.0.0-5.el6  
augeas-devel-1.0.0-5.el6

#### 181115 - FreeBSD OpenTTD Denial Of Service Using Forcefully Crashed Aircrafts (d2073237-5b52-11e3-80f7-c86000c6ec)

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

Risk Level: Low

CVE: CVE-2013-6411

#### Description

The scan detected that the host is missing the following update: OpenTTD -- Denial of service using forcefully crashed aircrafts (d2073237-5b52-11e3-80f7-c86000cbc6ec)

#### Observation

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

<http://www.vuxml.org/freebsd/d2073237-5b52-11e3-80f7-c86000cbc6ec.html>

Affected packages:

0.3.6 <= openttd < 1.3.3

181116 - FreeBSD monitorix Serious Bug In The Built-in HTTP Server (620cf713-5a99-11e3-878d-20cf30e32f6d)

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

Risk Level: Low

#### Description

The scan detected that the host is missing the following update: monitorix -- serious bug in the built-in HTTP server (620cf713-5a99-11e3-878d-20cf30e32f6d)

#### Observation

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

<http://www.vuxml.org/freebsd/620cf713-5a99-11e3-878d-20cf30e32f6d.html>

Affected packages:

monitorix < 3.3.1

184229 - Ubuntu Linux 12.04, 12.10, 13.04, 13.10 USN-2047-1 Update Is Not Installed

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

Risk Level: Low

#### Description

The scan detected that the host is missing the following update: USN-2047-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2013-December/002335.html>

Ubuntu 12.10

libpixmap-1-0\_0.26.0-3ubuntu0.1

Ubuntu 13.10

libpixmap-1-0\_0.30.2-1ubuntu0.1

Ubuntu 12.04

libpixmap-1-0\_0.24.4-1ubuntu0.1



Ubuntu 13.04

libpixmap-1-0\_0.28.2-0ubuntu1.1

#### 187356 - Fedora Linux 19 FEDORA-2013-21856 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4567, CVE-2013-4568, CVE-2013-4572

##### Description

The scan detected that the host is missing the following update: FEDORA-2013-21856

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123011.html>

Fedora Core 19

mediawiki-1.21.3-1.fc19

#### 187357 - Fedora Linux 18 FEDORA-2013-21874 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-4567, CVE-2013-4568, CVE-2013-4572

##### Description

The scan detected that the host is missing the following update: FEDORA-2013-21874

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/122998.html>

Fedora Core 18

mediawiki-1.19.9-1.fc18

#### 187359 - Fedora Linux 20 FEDORA-2013-22168 Update Is Not Installed

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

Risk Level: Low

##### Description

The scan detected that the host is missing the following update: FEDORA-2013-22168

##### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2013-November/122929.html>

Fedora Core 20

gnome-shell-3.10.2.1-2.fc20

### 187361 - Fedora Linux 19 FEDORA-2013-21844 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2013-6385, CVE-2013-6386, CVE-2013-6387, CVE-2013-6388, CVE-2013-6389

#### Description

The scan detected that the host is missing the following update: FEDORA-2013-21844

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2013-December/123015.html>

Fedora Core 19

drupal7-7.24-1.fc19

## 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.

### 13385 - Mozilla Bugzilla XML-RPC API Cross Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-0453

#### Update Details

Recommendation is updated.

### 15619 - Cisco Prime Network Control System (NCS) Health Monitor Login Page Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2012-5990

#### Update Details

Recommendation is updated.

## 15741 - Cisco AnyConnect Secure Mobility Client Library Directory Local Privilege Escalation

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-1130

### Update Details

Recommendation is updated.

## 15988 - Microsoft Windows NDProxy Privilege Escalation (2914486)

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

Risk Level: Medium

CVE: CVE-2013-5065

Microsoft ID: 2914486

### Update Details

Description is updated.

Observation is updated.

## 95873 - SuSE SLES 11, 11 SP3, SLED 11, 11 SP3 kernel-8528 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-2206

### Update Details

FASLScript is updated.

## 32784 - Sun Solaris 145712-07 Update Is Not Installed

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

Risk Level: Low

### Update Details

Name is updated.

Description is updated.

Observation is updated.

Recommendation is updated.

FASLScript is updated.

## 32785 - Sun Solaris 145711-07 Update Is Not Installed

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

Risk Level: Low

### Update Details

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

## ADDITIONAL NOTES

1 - Risk Score for Shell/Unix Patch Content has been aligned to CVSS ranges. Further details can be found on the CSV file included in this release

## HOW TO UPDATE

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

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

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

## MCAFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

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 2012 McAfee, Inc.

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