

## 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

#### 141432 - Red Hat Enterprise Linux RHSA-2017-0307 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6136, CVE-2016-9555

#### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0307

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0307.html>

#### RHEL6D

i386  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6

#### noarch

kernel-firmware-2.6.32-642.15.1.el6  
kernel-doc-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6

#### x86\_64

kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-debuginfo-2.6.32-642.15.1.el6

kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6

## RHEL6S

i386  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6

## noarch

kernel-firmware-2.6.32-642.15.1.el6  
kernel-doc-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6

## x86\_64

kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6

## RHEL6WS

i386  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6

## noarch

kernel-firmware-2.6.32-642.15.1.el6  
kernel-doc-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6

## x86\_64

kernel-debuginfo-common-x86\_64-2.6.32-642.15.1.el6  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6

## 145237 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0575-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8709, CVE-2016-7117, CVE-2016-9806, CVE-2017-2583, CVE-2017-2584, CVE-2017-5551, CVE-2017-5576, CVE-2017-5577, CVE-2017-5897, CVE-2017-5970, CVE-2017-5986

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0575-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002668.html>

### SuSE SLED 12 SP2

x86\_64  
kernel-default-extra-4.4.49-92.11.1  
kernel-default-debuginfo-4.4.49-92.11.1  
kernel-default-devel-4.4.49-92.11.1  
kernel-default-4.4.49-92.11.1  
kernel-default-extra-debuginfo-4.4.49-92.11.1  
kernel-syms-4.4.49-92.11.1  
kernel-default-debugsource-4.4.49-92.11.1

### noarch

kernel-macros-4.4.49-92.11.1  
kernel-source-4.4.49-92.11.1  
kernel-devel-4.4.49-92.11.1

### SuSE SLES 12 SP2

noarch  
kernel-macros-4.4.49-92.11.1  
kernel-source-4.4.49-92.11.1  
kernel-devel-4.4.49-92.11.1

### x86\_64

kernel-default-debuginfo-4.4.49-92.11.1  
kernel-default-devel-4.4.49-92.11.1  
kernel-default-4.4.49-92.11.1  
kernel-syms-4.4.49-92.11.1  
kernel-default-base-debuginfo-4.4.49-92.11.1  
kernel-default-base-4.4.49-92.11.1

## 160213 - CentOS 6 CESA-2017-0307 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6136, CVE-2016-9555

### Description

The scan detected that the host is missing the following update:  
CESA-2017-0307

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-February/022281.html>

CentOS 6

i686

kernel-devel-2.6.32-642.15.1.el6

kernel-debug-2.6.32-642.15.1.el6

kernel-2.6.32-642.15.1.el6

kernel-headers-2.6.32-642.15.1.el6

perf-2.6.32-642.15.1.el6

python-perf-2.6.32-642.15.1.el6

kernel-debug-devel-2.6.32-642.15.1.el6

noarch

kernel-firmware-2.6.32-642.15.1.el6

kernel-doc-2.6.32-642.15.1.el6

kernel-abi-whitelists-2.6.32-642.15.1.el6

x86\_64

kernel-devel-2.6.32-642.15.1.el6

kernel-debug-2.6.32-642.15.1.el6

kernel-2.6.32-642.15.1.el6

kernel-headers-2.6.32-642.15.1.el6

perf-2.6.32-642.15.1.el6

python-perf-2.6.32-642.15.1.el6

kernel-debug-devel-2.6.32-642.15.1.el6

## 163287 - Oracle Enterprise Linux ELSA-2017-0307 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6136, CVE-2016-9555, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0307

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006723.html>

## OEL6

x86\_64

kernel-doc-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
kernel-firmware-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6

i386

kernel-doc-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
kernel-firmware-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6

## 170777 - Amazon Linux AMI ALAS-2017-800 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5616, CVE-2016-6662, CVE-2016-6663

### Description

The scan detected that the host is missing the following update:  
ALAS-2017-800

### Observation

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

<https://alas.aws.amazon.com/ALAS-2017-800.html>

## Amazon Linux AMI

x86\_64

mysql51-embedded-5.1.73-8.72.amzn1  
mysql51-devel-5.1.73-8.72.amzn1  
mysql51-test-5.1.73-8.72.amzn1  
mysql51-embedded-devel-5.1.73-8.72.amzn1  
mysql51-5.1.73-8.72.amzn1  
mysql51-server-5.1.73-8.72.amzn1  
mysql51-debuginfo-5.1.73-8.72.amzn1  
mysql51-libs-5.1.73-8.72.amzn1  
mysql51-bench-5.1.73-8.72.amzn1  
mysql51-common-5.1.73-8.72.amzn1

i686

mysql51-embedded-5.1.73-8.72.amzn1

mysql51-devel-5.1.73-8.72.amzn1  
mysql51-test-5.1.73-8.72.amzn1  
mysql51-embedded-devel-5.1.73-8.72.amzn1  
mysql51-bench-5.1.73-8.72.amzn1  
mysql51-libs-5.1.73-8.72.amzn1  
mysql51-server-5.1.73-8.72.amzn1  
mysql51-debuginfo-5.1.73-8.72.amzn1  
mysql51-5.1.73-8.72.amzn1  
mysql51-common-5.1.73-8.72.amzn1

## 175116 - Scientific Linux Security ERRATA Moderate: kernel on SL6.x i386/x86\_64 (1702-4925)

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

Risk Level: High

CVE: CVE-2016-6136, CVE-2016-9555

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Moderate: kernel on SL6.x i386/x86\_64 (1702-4925)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1702&L=scientific-linux-errata&F=&S=&P=4925>

SL6

i386

kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6  
kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6

noarch

kernel-firmware-2.6.32-642.15.1.el6  
kernel-doc-2.6.32-642.15.1.el6  
kernel-abi-whitelists-2.6.32-642.15.1.el6

x86\_64

kernel-debug-debuginfo-2.6.32-642.15.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.15.1.el6  
python-perf-2.6.32-642.15.1.el6  
python-perf-debuginfo-2.6.32-642.15.1.el6  
kernel-debug-devel-2.6.32-642.15.1.el6  
kernel-debug-2.6.32-642.15.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.15.1.el6  
kernel-devel-2.6.32-642.15.1.el6  
kernel-debuginfo-2.6.32-642.15.1.el6  
kernel-headers-2.6.32-642.15.1.el6  
perf-2.6.32-642.15.1.el6

perf-debuginfo-2.6.32-642.15.1.el6  
kernel-2.6.32-642.15.1.el6

## 130708 - Debian Linux 8.0 DSA-3791-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6786, CVE-2016-6787, CVE-2016-8405, CVE-2016-9191, CVE-2017-2583, CVE-2017-2584, CVE-2017-2596, CVE-2017-2618, CVE-2017-5549, CVE-2017-5551, CVE-2017-5897, CVE-2017-5970, CVE-2017-6001, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
DSA-3791-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3791>

Debian 8.0

all

acpi-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
nic-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
scsi-core-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
linux-headers-3.16.0-4-powerpc-smp\_3.16.39-1+deb8u1  
ext4-modules-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1  
nic-wireless-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
btrfs-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
fat-modules-3.16.0-4-versatile-di\_3.16.39-1+deb8u1  
multipath-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-arm64-dbg\_3.16.39-1+deb8u1  
cdrom-core-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
jfs-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
btrfs-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
jfs-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
loop-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
nic-pcmcia-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
crypto-modules-3.16.0-4-armmp-di\_3.16.39-1+deb8u1  
scsi-extra-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
zlib-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
nic-wireless-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
acpi-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
nbd-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-r5k-ip32\_3.16.39-1+deb8u1  
nbd-modules-3.16.0-4-r5k-ip32-di\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-armmp-di\_3.16.39-1+deb8u1  
md-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
virtio-modules-3.16.0-4-powerpc64le-di\_3.16.39-1+deb8u1  
linux-headers-3.16.0-4-orion5x\_3.16.39-1+deb8u1  
fuse-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
affs-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
usb-storage-modules-3.16.0-4-versatile-di\_3.16.39-1+deb8u1  
crypto-modules-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1  
kernel-image-3.16.0-4-r5k-ip32-di\_3.16.39-1+deb8u1  
pcmcia-storage-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
ntfs-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
nic-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1

input-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
multipath-modules-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1  
sata-modules-3.16.0-4-armmp-di\_3.16.39-1+deb8u1  
xfs-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
scsi-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
isofs-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
firewire-core-modules-3.16.0-4-powerpc64le-di\_3.16.39-1+deb8u1  
crc-modules-3.16.0-4-r5k-ip32-di\_3.16.39-1+deb8u1  
sata-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
nic-shared-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
mouse-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
isofs-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
fb-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
event-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
btrfs-modules-3.16.0-4-orion5x-di\_3.16.39-1+deb8u1  
uinput-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
crypto-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
jfs-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
serial-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
uinput-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-686-pae\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-armmp\_3.16.39-1+deb8u1  
pcmcia-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
nic-shared-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
kernel-image-3.16.0-4-s390x-di\_3.16.39-1+deb8u1  
ppp-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1  
sata-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
ntfs-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
usb-storage-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-amd64-dbg\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1  
kernel-image-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1  
cdrom-core-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
core-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
scsi-core-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
cdrom-core-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
scsi-common-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1  
loop-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
mouse-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
pata-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
pcmcia-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
crypto-dm-modules-3.16.0-4-armmp-di\_3.16.39-1+deb8u1  
pcmcia-storage-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
xfs-modules-3.16.0-4-s390x-di\_3.16.39-1+deb8u1  
scsi-common-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
scsi-modules-3.16.0-4-powerpc64le-di\_3.16.39-1+deb8u1  
ntfs-modules-3.16.0-4-loongson-2f-di\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-powerpc64le-di\_3.16.39-1+deb8u1  
nbd-modules-3.16.0-4-r4k-ip22-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-586\_3.16.39-1+deb8u1  
usb-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
affs-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
sata-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
linux-headers-3.16.0-4-all-armel\_3.16.39-1+deb8u1  
udf-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
cdrom-core-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
minix-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
pata-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
input-modules-3.16.0-4-armmp-di\_3.16.39-1+deb8u1  
linux-image-3.16.0-4-loongson-2e\_3.16.39-1+deb8u1



nic-wireless-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
crypto-modules-3.16.0-4-r5k-ip32-di\_3.16.39-1+deb8u1  
kernel-image-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
event-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
input-modules-3.16.0-4-arm64-di\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
linux-headers-3.16.0-4-kirkwood\_3.16.39-1+deb8u1  
crypto-dm-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
minix-modules-3.16.0-4-octeon-di\_3.16.39-1+deb8u1  
xfs-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
crypto-dm-modules-3.16.0-4-s390x-di\_3.16.39-1+deb8u1  
nbd-modules-3.16.0-4-amd64-di\_3.16.39-1+deb8u1  
virtio-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
pata-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
serial-modules-3.16.0-4-powerpc-di\_3.16.39-1+deb8u1  
affs-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
squashfs-modules-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1  
usb-serial-modules-3.16.0-4-powerpc64le-di\_3.16.39-1+deb8u1  
linux-headers-3.16.0-4-arm64\_3.16.39-1+deb8u1  
crypto-dm-modules-3.16.0-4-loongson-2e-di\_3.16.39-1+deb8u1  
kernel-image-3.16.0-4-arm64-di\_3.16.39-1+deb8u1  
md-modules-3.16.0-4-s390x-di\_3.16.39-1+deb8u1  
i2c-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
cdrom-core-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
crypto-dm-modules-3.16.0-4-loongson-3-di\_3.16.39-1+deb8u1  
ntfs-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
scsi-common-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
firewire-core-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
scsi-extra-modules-3.16.0-4-powerpc64-di\_3.16.39-1+deb8u1  
pcmcia-storage-modules-3.16.0-4-586-di\_3.16.39-1+deb8u1  
nbd-modules-3.16.0-4-686-pae-di\_3.16.39-1+deb8u1  
i2c-modules-3.16.0-4-4kc-malta-di\_3.16.39-1+deb8u1  
udf-modules-3.16.0-4-sb1-bcm91250a-di\_3.16.39-1+deb8u1  
mmc-modules-3.16.0-4-kirkwood-di\_3.16.39-1+deb8u1

## 132339 - Oracle VM OVMSA-2017-0045 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

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

OVMSA-2017-0045

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-February/000654.html>

OVM3.3

x86\_64

kernel-uek-3.8.13-118.16.4.el6uek

kernel-uek-firmware-3.8.13-118.16.4.el6uek

## 132340 - Oracle VM OVMSA-2017-0044 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
OVMSA-2017-0044

### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-February/000653.html>

OVM3.4  
x86\_64  
kernel-uek-firmware-4.1.12-61.1.28.el6uek  
kernel-uek-4.1.12-61.1.28.el6uek

## 132342 - Oracle VM OVMSA-2017-0046 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
OVMSA-2017-0046

### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-February/000655.html>

OVM3.2  
x86\_64  
kernel-uek-2.6.39-400.294.3.el5uek  
kernel-uek-firmware-2.6.39-400.294.3.el5uek

## 141428 - Red Hat Enterprise Linux RHSA-2017-0294 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0294

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0294.html>

#### RHEL7D

x86\_64  
kernel-3.10.0-514.6.2.el7  
perf-3.10.0-514.6.2.el7  
kernel-debuginfo-common-x86\_64-3.10.0-514.6.2.el7  
kernel-debug-debuginfo-3.10.0-514.6.2.el7  
kernel-tools-libs-devel-3.10.0-514.6.2.el7  
kernel-headers-3.10.0-514.6.2.el7  
perf-debuginfo-3.10.0-514.6.2.el7  
kernel-debuginfo-3.10.0-514.6.2.el7  
kernel-devel-3.10.0-514.6.2.el7  
kernel-tools-libs-3.10.0-514.6.2.el7  
kernel-debug-devel-3.10.0-514.6.2.el7  
kernel-tools-debuginfo-3.10.0-514.6.2.el7  
kernel-tools-3.10.0-514.6.2.el7  
python-perf-debuginfo-3.10.0-514.6.2.el7  
python-perf-3.10.0-514.6.2.el7  
kernel-debug-3.10.0-514.6.2.el7

#### noarch

kernel-doc-3.10.0-514.6.2.el7  
kernel-abi-whitelists-3.10.0-514.6.2.el7

#### RHEL7S

noarch  
kernel-doc-3.10.0-514.6.2.el7  
kernel-abi-whitelists-3.10.0-514.6.2.el7

#### RHEL7WS

x86\_64  
kernel-3.10.0-514.6.2.el7  
perf-3.10.0-514.6.2.el7  
kernel-debuginfo-common-x86\_64-3.10.0-514.6.2.el7  
kernel-debug-debuginfo-3.10.0-514.6.2.el7  
kernel-tools-libs-devel-3.10.0-514.6.2.el7  
kernel-headers-3.10.0-514.6.2.el7  
perf-debuginfo-3.10.0-514.6.2.el7  
kernel-debuginfo-3.10.0-514.6.2.el7  
kernel-devel-3.10.0-514.6.2.el7  
kernel-tools-libs-3.10.0-514.6.2.el7  
kernel-debug-devel-3.10.0-514.6.2.el7  
kernel-tools-debuginfo-3.10.0-514.6.2.el7  
kernel-tools-3.10.0-514.6.2.el7  
python-perf-debuginfo-3.10.0-514.6.2.el7  
python-perf-3.10.0-514.6.2.el7  
kernel-debug-3.10.0-514.6.2.el7

#### noarch

kernel-doc-3.10.0-514.6.2.el7  
kernel-abi-whitelists-3.10.0-514.6.2.el7

### 141429 - Red Hat Enterprise Linux RHSA-2017-0323 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0323

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0323.html>

#### RHEL5D

i386

kernel-xen-devel-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-PAE-devel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-PAE-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-2.6.18-419.el5  
kernel-PAE-debuginfo-2.6.18-419.el5

noarch

kernel-doc-2.6.18-419.el5

x86\_64

kernel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-xen-devel-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5

#### RHEL5S

noarch

kernel-doc-2.6.18-419.el5

x86\_64

kernel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-xen-devel-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5

kernel-debug-devel-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5

i386

kernel-xen-devel-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-PAE-devel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-PAE-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-2.6.18-419.el5  
kernel-PAE-debuginfo-2.6.18-419.el5

## 141434 - Red Hat Enterprise Linux RHSA-2017-0293 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0293

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0293.html>

RHEL6D

i386  
kernel-devel-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

noarch

kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6

x86\_64

perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6

python-perf-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
kernel-devel-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

## RHEL6S

i386  
kernel-devel-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

## noarch

kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6

## x86\_64

perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
kernel-devel-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

## RHEL6WS

i386  
kernel-devel-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

noarch  
kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6

x86\_64  
kernel-devel-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

## 160214 - CentOS 5 CESA-2017-0323 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
CESA-2017-0323

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-February/022293.html>

CentOS 5  
i386  
kernel-headers-2.6.18-419.el5

i686  
kernel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-xen-devel-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-PAE-devel-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-PAE-2.6.18-419.el5

noarch  
kernel-doc-2.6.18-419.el5

x86\_64  
kernel-2.6.18-419.el5  
kernel-xen-devel-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5

kernel-xen-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5

## 160215 - CentOS 7 CESA-2017-0294 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
CESA-2017-0294

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-February/022280.html>

CentOS 7  
x86\_64  
kernel-tools-libs-devel-3.10.0-514.6.2.el7  
kernel-debug-devel-3.10.0-514.6.2.el7  
kernel-debug-3.10.0-514.6.2.el7  
kernel-tools-3.10.0-514.6.2.el7  
kernel-3.10.0-514.6.2.el7  
python-perf-3.10.0-514.6.2.el7  
kernel-headers-3.10.0-514.6.2.el7  
kernel-tools-libs-3.10.0-514.6.2.el7  
kernel-devel-3.10.0-514.6.2.el7  
perf-3.10.0-514.6.2.el7

noarch  
kernel-doc-3.10.0-514.6.2.el7  
kernel-abi-whitelists-3.10.0-514.6.2.el7

## 160216 - CentOS 6 CESA-2017-0293 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
CESA-2017-0293

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-February/022279.html>

CentOS 6  
i686  
kernel-devel-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6



kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6

noarch  
kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6

x86\_64  
kernel-devel-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6

## 163283 - Oracle Enterprise Linux ELSA-2017-3522 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-3522

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006732.html>  
<http://oss.oracle.com/pipermail/el-errata/2017-February/006733.html>

OEL5  
x86\_64  
kernel-uek-2.6.39-400.294.3.el5uek  
kernel-uek-debug-2.6.39-400.294.3.el5uek  
kernel-uek-doc-2.6.39-400.294.3.el5uek  
kernel-uek-firmware-2.6.39-400.294.3.el5uek  
kernel-uek-devel-2.6.39-400.294.3.el5uek  
kernel-uek-debug-devel-2.6.39-400.294.3.el5uek

i386  
kernel-uek-debug-2.6.39-400.294.3.el5uek  
kernel-uek-doc-2.6.39-400.294.3.el5uek  
kernel-uek-firmware-2.6.39-400.294.3.el5uek  
kernel-uek-devel-2.6.39-400.294.3.el5uek  
kernel-uek-debug-devel-2.6.39-400.294.3.el5uek  
kernel-uek-2.6.39-400.294.3.el5uek

OEL6  
x86\_64  
kernel-uek-debug-devel-2.6.39-400.294.3.el6uek  
kernel-uek-devel-2.6.39-400.294.3.el6uek

kernel-uek-2.6.39-400.294.3.el6uek  
kernel-uek-doc-2.6.39-400.294.3.el6uek  
kernel-uek-firmware-2.6.39-400.294.3.el6uek  
kernel-uek-debug-2.6.39-400.294.3.el6uek

i386

kernel-uek-debug-devel-2.6.39-400.294.3.el6uek  
kernel-uek-devel-2.6.39-400.294.3.el6uek  
kernel-uek-2.6.39-400.294.3.el6uek  
kernel-uek-doc-2.6.39-400.294.3.el6uek  
kernel-uek-firmware-2.6.39-400.294.3.el6uek  
kernel-uek-debug-2.6.39-400.294.3.el6uek

## 163284 - Oracle Enterprise Linux ELSA-2017-3520 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

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

ELSA-2017-3520

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2017-February/006730.html>

<http://oss.oracle.com/pipermail/el-errata/2017-February/006731.html>

OEL7

x86\_64

kernel-uek-debug-devel-4.1.12-61.1.28.el7uek  
kernel-uek-doc-4.1.12-61.1.28.el7uek  
kernel-uek-devel-4.1.12-61.1.28.el7uek  
dtrace-modules-4.1.12-61.1.28.el7uek-0.5.3-2.el7  
kernel-uek-firmware-4.1.12-61.1.28.el7uek  
kernel-uek-debug-4.1.12-61.1.28.el7uek  
kernel-uek-4.1.12-61.1.28.el7uek

OEL6

x86\_64

kernel-uek-doc-4.1.12-61.1.28.el6uek  
dtrace-modules-4.1.12-61.1.28.el6uek-0.5.3-2.el6  
kernel-uek-firmware-4.1.12-61.1.28.el6uek  
kernel-uek-devel-4.1.12-61.1.28.el6uek  
kernel-uek-4.1.12-61.1.28.el6uek  
kernel-uek-debug-4.1.12-61.1.28.el6uek  
kernel-uek-debug-devel-4.1.12-61.1.28.el6uek

## 163285 - Oracle Enterprise Linux ELSA-2017-0294 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0294

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006718.html>  
<http://oss.oracle.com/pipermail/el-errata/2017-February/006716.html>

#### OEL7

x86\_64  
kernel-doc-3.10.0-514.6.2.el7  
python-perf-3.10.0-514.6.2.0.1.el7  
kernel-tools-libs-3.10.0-514.6.2.0.1.el7  
kernel-3.10.0-514.6.2.el7  
perf-3.10.0-514.6.2.el7  
kernel-debug-devel-3.10.0-514.6.2.0.1.el7  
kernel-debug-3.10.0-514.6.2.0.1.el7  
kernel-tools-libs-devel-3.10.0-514.6.2.el7  
kernel-headers-3.10.0-514.6.2.0.1.el7  
kernel-abi-whitelists-3.10.0-514.6.2.el7  
kernel-headers-3.10.0-514.6.2.el7  
kernel-doc-3.10.0-514.6.2.0.1.el7  
kernel-devel-3.10.0-514.6.2.el7  
kernel-tools-libs-3.10.0-514.6.2.el7  
kernel-debug-devel-3.10.0-514.6.2.el7  
kernel-abi-whitelists-3.10.0-514.6.2.0.1.el7  
kernel-tools-3.10.0-514.6.2.el7  
kernel-3.10.0-514.6.2.0.1.el7  
kernel-tools-3.10.0-514.6.2.0.1.el7  
kernel-tools-libs-devel-3.10.0-514.6.2.0.1.el7  
kernel-devel-3.10.0-514.6.2.0.1.el7  
python-perf-3.10.0-514.6.2.el7  
perf-3.10.0-514.6.2.0.1.el7  
kernel-debug-3.10.0-514.6.2.el7

### 163286 - Oracle Enterprise Linux ELSA-2017-0293 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0293

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006717.html>

#### OEL6

x86\_64  
kernel-devel-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6

python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6

i386  
kernel-devel-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6

## 163288 - Oracle Enterprise Linux ELSA-2017-0323 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0323

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006739.html>

<http://oss.oracle.com/pipermail/el-errata/2017-February/006740.html>

### OEL5

i386  
kernel-xen-devel-2.6.18-419.el5  
kernel-PAE-devel-2.6.18-419.el5  
kernel-PAE-2.6.18-419.0.0.1.el5  
kernel-xen-devel-2.6.18-419.0.0.1.el5  
kernel-xen-2.6.18-419.el5  
kernel-xen-2.6.18-419.0.0.1.el5  
kernel-PAE-2.6.18-419.el5  
kernel-2.6.18-419.0.0.1.el5  
kernel-debug-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-doc-2.6.18-419.el5  
kernel-headers-2.6.18-419.0.0.1.el5  
kernel-doc-2.6.18-419.0.0.1.el5  
kernel-devel-2.6.18-419.el5  
kernel-devel-2.6.18-419.0.0.1.el5  
kernel-debug-2.6.18-419.0.0.1.el5  
kernel-2.6.18-419.el5

kernel-PAE-devel-2.6.18-419.0.0.1.el5  
kernel-debug-devel-2.6.18-419.0.0.1.el5

x86\_64  
kernel-xen-devel-2.6.18-419.el5  
kernel-doc-2.6.18-419.0.0.1.el5  
kernel-xen-devel-2.6.18-419.0.0.1.el5  
kernel-xen-2.6.18-419.el5  
kernel-xen-2.6.18-419.0.0.1.el5  
kernel-2.6.18-419.0.0.1.el5  
kernel-debug-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-doc-2.6.18-419.el5  
kernel-headers-2.6.18-419.0.0.1.el5  
kernel-devel-2.6.18-419.el5  
kernel-devel-2.6.18-419.0.0.1.el5  
kernel-debug-2.6.18-419.0.0.1.el5  
kernel-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.0.0.1.el5

## 163290 - Oracle Enterprise Linux ELSA-2017-3521 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-3521

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006735.html>  
<http://oss.oracle.com/pipermail/el-errata/2017-February/006734.html>

OEL7  
x86\_64  
kernel-uek-devel-3.8.13-118.16.4.el7uek  
kernel-uek-debug-devel-3.8.13-118.16.4.el7uek  
kernel-uek-debug-3.8.13-118.16.4.el7uek  
kernel-uek-doc-3.8.13-118.16.4.el7uek  
kernel-uek-3.8.13-118.16.4.el7uek  
kernel-uek-firmware-3.8.13-118.16.4.el7uek  
dtrace-modules-3.8.13-118.16.4.el7uek-0.4.5-3.el7

OEL6  
x86\_64  
dtrace-modules-3.8.13-118.16.4.el6uek-0.4.5-3.el6  
kernel-uek-doc-3.8.13-118.16.4.el6uek  
kernel-uek-devel-3.8.13-118.16.4.el6uek  
kernel-uek-3.8.13-118.16.4.el6uek  
kernel-uek-debug-3.8.13-118.16.4.el6uek  
kernel-uek-debug-devel-3.8.13-118.16.4.el6uek  
kernel-uek-firmware-3.8.13-118.16.4.el6uek

## 175117 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86\_64 (1702-4279)

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: kernel on SL7.x x86\_64 (1702-4279)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1702&L=scientific-linux-errata&F=&S=&P=4279>

SL7

x86\_64

kernel-3.10.0-514.6.2.el7

perf-3.10.0-514.6.2.el7

kernel-debuginfo-common-x86\_64-3.10.0-514.6.2.el7

kernel-debug-debuginfo-3.10.0-514.6.2.el7

kernel-tools-libs-devel-3.10.0-514.6.2.el7

kernel-headers-3.10.0-514.6.2.el7

perf-debuginfo-3.10.0-514.6.2.el7

kernel-debuginfo-3.10.0-514.6.2.el7

kernel-devel-3.10.0-514.6.2.el7

kernel-tools-libs-3.10.0-514.6.2.el7

kernel-debug-devel-3.10.0-514.6.2.el7

kernel-tools-debuginfo-3.10.0-514.6.2.el7

kernel-tools-3.10.0-514.6.2.el7

python-perf-debuginfo-3.10.0-514.6.2.el7

python-perf-3.10.0-514.6.2.el7

kernel-debug-3.10.0-514.6.2.el7

noarch

kernel-doc-3.10.0-514.6.2.el7

kernel-abi-whitelists-3.10.0-514.6.2.el7

## 175119 - Scientific Linux Security ERRATA Important: kernel on SL5.x i386/x86\_64 (1702-5638)

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

Risk Level: High

CVE: CVE-2017-2634, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: kernel on SL5.x i386/x86\_64 (1702-5638)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1702&L=scientific-linux-errata&F=&S=&P=5638>

SL5

i386  
kernel-xen-devel-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-PAE-devel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-PAE-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-2.6.18-419.el5  
kernel-PAE-debuginfo-2.6.18-419.el5

noarch  
kernel-doc-2.6.18-419.el5

x86\_64  
kernel-2.6.18-419.el5  
kernel-xen-2.6.18-419.el5  
kernel-headers-2.6.18-419.el5  
kernel-xen-devel-2.6.18-419.el5  
kernel-debuginfo-common-2.6.18-419.el5  
kernel-debug-2.6.18-419.el5  
kernel-xen-debuginfo-2.6.18-419.el5  
kernel-devel-2.6.18-419.el5  
kernel-debug-debuginfo-2.6.18-419.el5  
kernel-debug-devel-2.6.18-419.el5  
kernel-debuginfo-2.6.18-419.el5

## 175120 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86\_64 (1702-4599)

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: kernel on SL6.x i386/x86\_64 (1702-4599)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1702&L=scientific-linux-errata&F=&S=&P=4599>

SL6  
i386  
kernel-devel-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6

kernel-debug-debuginfo-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

noarch  
kernel-abi-whitelists-2.6.32-642.13.2.el6  
kernel-doc-2.6.32-642.13.2.el6  
kernel-firmware-2.6.32-642.13.2.el6

x86\_64  
perf-debuginfo-2.6.32-642.13.2.el6  
kernel-debuginfo-2.6.32-642.13.2.el6  
python-perf-2.6.32-642.13.2.el6  
perf-2.6.32-642.13.2.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.13.2.el6  
kernel-debug-debuginfo-2.6.32-642.13.2.el6  
kernel-2.6.32-642.13.2.el6  
kernel-headers-2.6.32-642.13.2.el6  
kernel-debug-devel-2.6.32-642.13.2.el6  
kernel-devel-2.6.32-642.13.2.el6  
kernel-debug-2.6.32-642.13.2.el6  
kernel-debuginfo-common-i686-2.6.32-642.13.2.el6  
python-perf-debuginfo-2.6.32-642.13.2.el6

## 185595 - Ubuntu Linux 16.04 USN-3208-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-9191, CVE-2016-9588, CVE-2017-2583, CVE-2017-2584, CVE-2017-5549, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
USN-3208-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003744.html>

Ubuntu 16.04

linux-image-generic\_4.4.0.64.68  
linux-image-powerpc-smp\_4.4.0.64.68  
linux-image-4.4.0-64-powerpc64-smp\_4.4.0-64.85  
linux-image-4.4.0-64-lowlatency\_4.4.0-64.85  
linux-image-4.4.0-64-powerpc64-emb\_4.4.0-64.85  
linux-image-powerpc-e500mc\_4.4.0.64.68  
linux-image-4.4.0-1048-snapdragon\_4.4.0-1048.52  
linux-image-snapdragon\_4.4.0.1048.40  
linux-image-generic-lpae\_4.4.0.64.68  
linux-image-4.4.0-64-generic\_4.4.0-64.85  
linux-image-4.4.0-64-generic-lpae\_4.4.0-64.85  
linux-image-4.4.0-64-powerpc-smp\_4.4.0-64.85  
linux-image-powerpc64-smp\_4.4.0.64.68  
linux-image-powerpc64-emb\_4.4.0.64.68  
linux-image-4.4.0-64-powerpc-e500mc\_4.4.0-64.85



linux-image-lowlatency\_4.4.0.64.68

### 185596 - Ubuntu Linux 12.04 USN-3207-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2016-7911, CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
USN-3207-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003743.html>

Ubuntu 12.04

linux-image-generic-lts-trusty\_3.13.0.110.101  
linux-image-generic-lpae-lts-trusty\_3.13.0.110.101  
linux-image-3.13.0-110-generic\_3.13.0-110.157~precise1  
linux-image-3.13.0-110-generic-lpae\_3.13.0-110.157~precise1

### 185597 - Ubuntu Linux 16.10 USN-3209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-9588, CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
USN-3209-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003746.html>

Ubuntu 16.10

linux-image-4.8.0-39-powerpc64-emb\_4.8.0-39.42  
linux-image-4.8.0-39-powerpc-smp\_4.8.0-39.42  
linux-image-lowlatency\_4.8.0.39.50  
linux-image-4.8.0-39-lowlatency\_4.8.0-39.42  
linux-image-raspi2\_4.8.0.1026.29  
linux-image-4.8.0-39-generic-lpae\_4.8.0-39.42  
linux-image-powerpc-smp\_4.8.0.39.50  
linux-image-4.8.0-39-generic\_4.8.0-39.42  
linux-image-4.8.0-1026-raspi2\_4.8.0-1026.29  
linux-image-4.8.0-39-powerpc-e500mc\_4.8.0-39.42  
linux-image-powerpc-e500mc\_4.8.0.39.50  
linux-image-generic-lpae\_4.8.0.39.50  
linux-image-generic\_4.8.0.39.50

linux-image-powerpc64-emb\_4.8.0.39.50

### 185598 - Ubuntu Linux 12.04 USN-3206-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2016-7911, CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
USN-3206-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003741.html>

Ubuntu 12.04

linux-image-omap\_3.2.0.123.138  
linux-image-3.2.0-123-generic\_3.2.0-123.166  
linux-image-3.2.0-123-virtual\_3.2.0-123.166  
linux-image-omap4\_3.2.0.1501.96  
linux-image-3.2.0-1501-omap4\_3.2.0-1501.128  
linux-image-virtual\_3.2.0.123.138  
linux-image-3.2.0-123-highbank\_3.2.0-123.166  
linux-image-3.2.0-123-powerpc64-smp\_3.2.0-123.166  
linux-image-3.2.0-123-omap\_3.2.0-123.166  
linux-image-3.2.0-123-powerpc-smp\_3.2.0-123.166  
linux-image-highbank\_3.2.0.123.138  
linux-image-powerpc-smp\_3.2.0.123.138  
linux-image-generic\_3.2.0.123.138  
linux-image-powerpc64-smp\_3.2.0.123.138  
linux-image-3.2.0-123-generic-pae\_3.2.0-123.166  
linux-image-generic-pae\_3.2.0.123.138

### 185599 - Ubuntu Linux 14.04 USN-3208-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-9191, CVE-2016-9588, CVE-2017-2583, CVE-2017-2584, CVE-2017-5549, CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
USN-3208-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003745.html>

Ubuntu 14.04

linux-image-powerpc-smp-lts-xenial\_4.4.0.64.50

linux-image-generic-lpae-lts-xenial\_4.4.0.64.50  
linux-image-powerpc-e500mc-lts-xenial\_4.4.0.64.50  
linux-image-4.4.0-64-lowlatency\_4.4.0-64.85~14.04.1  
linux-image-lowlatency-lts-xenial\_4.4.0.64.50  
linux-image-4.4.0-64-powerpc64-emb\_4.4.0-64.85~14.04.1  
linux-image-4.4.0-64-powerpc-smp\_4.4.0-64.85~14.04.1  
linux-image-generic-lts-xenial\_4.4.0.64.50  
linux-image-4.4.0-64-generic-lpae\_4.4.0-64.85~14.04.1  
linux-image-4.4.0-64-powerpc-e500mc\_4.4.0-64.85~14.04.1  
linux-image-4.4.0-64-generic\_4.4.0-64.85~14.04.1  
linux-image-4.4.0-64-powerpc64-smp\_4.4.0-64.85~14.04.1  
linux-image-powerpc64-emb-lts-xenial\_4.4.0.64.50  
linux-image-powerpc64-smp-lts-xenial\_4.4.0.64.50

## 185601 - Ubuntu Linux 14.04 USN-3207-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7910, CVE-2016-7911, CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
USN-3207-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003742.html>

Ubuntu 14.04

linux-image-powerpc-e500mc\_3.13.0.110.118  
linux-image-3.13.0-110-powerpc64-emb\_3.13.0-110.157  
linux-image-powerpc64-emb\_3.13.0.110.118  
linux-image-3.13.0-110-lowlatency\_3.13.0-110.157  
linux-image-lowlatency\_3.13.0.110.118  
linux-image-powerpc-e500\_3.13.0.110.118  
linux-image-generic\_3.13.0.110.118  
linux-image-powerpc-smp\_3.13.0.110.118  
linux-image-3.13.0-110-powerpc-e500mc\_3.13.0-110.157  
linux-image-generic-lpae\_3.13.0.110.118  
linux-image-powerpc64-smp\_3.13.0.110.118  
linux-image-3.13.0-110-generic\_3.13.0-110.157  
linux-image-3.13.0-110-powerpc-smp\_3.13.0-110.157  
linux-image-highbank\_3.13.0.110.118  
linux-image-3.13.0-110-generic-lpae\_3.13.0-110.157  
linux-image-3.13.0-110-powerpc-e500\_3.13.0-110.157  
linux-image-3.13.0-110-powerpc64-smp\_3.13.0-110.157

## 191755 - Fedora Linux 25 FEDORA-2017-f519ebb3c4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6074

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-f519ebb3c4

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=1>

Fedora Core 25

kernel-4.9.12-200.fc25

### **191761 - Fedora Linux 24 FEDORA-2017-4b9f61c68d Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-6074

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-4b9f61c68d

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=1>

Fedora Core 24

kernel-4.9.12-100.fc24

### **21276 - (K01587042) F5 BIG-IP SPDY And HTTP2 Profile Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7475

#### Description

A vulnerability is present in some versions of F5's BIG-IP Products.

#### Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the Traffic Management Microkernel (TMM) component. Successful exploitation could allow an attacker to cause a denial of service condition.

### **21295 - Hughes Satellite Modems Multiple Vulnerabilities**

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

Risk Level: High

CVE: CVE-2016-9494, CVE-2016-9495, CVE-2016-9496, CVE-2016-9497

### Description

Multiple vulnerabilities are present in some versions of Hughes satellite modems.

### Observation

Hughes satellite provides satellite broadband for home and office.

Multiple vulnerabilities are present in some versions of Hughes satellite modems. The flaws lie in DW7000, HN7740S, and HN7000S/SM devices running software versions prior to 6.9.0.34. Successful exploitation could allow an attacker to cause a denial of service, bypass authentication or access some administrative commands with default credentials.

## **21296 - Advantech WebAccess DLL Hijacking Vulnerability Prior To 8.2**

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

Risk Level: High

CVE: CVE-2017-5175

### Description

A vulnerability is present in some versions of Advantech WebAccess.

### Observation

Advantech WebAccess is a web-based HMI software application used in energy, manufacturing, and building automation systems.

A vulnerability is present in some versions of Advantech WebAccess. The flaw is due to an uncontrolled search path element. Successful exploitation by an attacker could result in the execution of arbitrary code.

## **21299 - (K54211024) F5 BIG-IP OpenSSL Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-6304

### Description

A denial-of-service vulnerability is present in some versions of F5 BIG-IP systems.

### Observation

F5's BIG-IP products are network appliances that run 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 OpenSSL component. Successful exploitation could allow an attacker to cause a denial-of-service.

## **145234 - SuSE SLES 11 SP4 SUSE-SU-2017:0568-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-7478

### Description

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

SUSE-SU-2017:0568-1

### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002664.html>

SuSE SLES 11 SP4

i586

php53-zlib-5.3.17-101.1  
php53-gd-5.3.17-101.1  
php53-fastcgi-5.3.17-101.1  
php53-openssl-5.3.17-101.1  
php53-wddx-5.3.17-101.1  
php53-json-5.3.17-101.1  
php53-xmlrpc-5.3.17-101.1  
php53-soap-5.3.17-101.1  
php53-pcntl-5.3.17-101.1  
php53-xmlreader-5.3.17-101.1  
php53-bz2-5.3.17-101.1  
php53-iconv-5.3.17-101.1  
php53-dba-5.3.17-101.1  
php53-sysvshm-5.3.17-101.1  
php53-curl-5.3.17-101.1  
php53-bcmath-5.3.17-101.1  
php53-xsl-5.3.17-101.1  
php53-pdo-5.3.17-101.1  
php53-ldap-5.3.17-101.1  
php53-pgsql-5.3.17-101.1  
php53-gettext-5.3.17-101.1  
php53-dom-5.3.17-101.1  
php53-odbc-5.3.17-101.1  
php53-mysql-5.3.17-101.1  
php53-gmp-5.3.17-101.1  
php53-zip-5.3.17-101.1  
php53-calendar-5.3.17-101.1  
php53-sysvmsg-5.3.17-101.1  
php53-shmop-5.3.17-101.1  
php53-ftp-5.3.17-101.1  
php53-mbstring-5.3.17-101.1  
php53-5.3.17-101.1  
php53-snmp-5.3.17-101.1  
php53-fileinfo-5.3.17-101.1  
php53-intl-5.3.17-101.1  
php53-openssl-5.3.17-101.1  
php53-exif-5.3.17-101.1  
php53-pear-5.3.17-101.1  
php53-suhosin-5.3.17-101.1  
php53-sysvsem-5.3.17-101.1  
php53-xmlwriter-5.3.17-101.1  
php53-mcrypt-5.3.17-101.1  
php53-ctype-5.3.17-101.1  
php53-tokenizer-5.3.17-101.1  
apache2-mod\_php53-5.3.17-101.1

x86\_64

php53-zlib-5.3.17-101.1  
php53-gd-5.3.17-101.1  
php53-fastcgi-5.3.17-101.1  
php53-openssl-5.3.17-101.1  
php53-wddx-5.3.17-101.1  
php53-json-5.3.17-101.1  
php53-xmlrpc-5.3.17-101.1

php53-soap-5.3.17-101.1  
php53-pcntl-5.3.17-101.1  
php53-xmlreader-5.3.17-101.1  
php53-bz2-5.3.17-101.1  
php53-iconv-5.3.17-101.1  
php53-dba-5.3.17-101.1  
php53-sysvshm-5.3.17-101.1  
php53-curl-5.3.17-101.1  
php53-bcmath-5.3.17-101.1  
php53-xsl-5.3.17-101.1  
php53-pdo-5.3.17-101.1  
php53-ldap-5.3.17-101.1  
php53-pgsql-5.3.17-101.1  
php53-gettext-5.3.17-101.1  
php53-dom-5.3.17-101.1  
php53-odbc-5.3.17-101.1  
php53-mysql-5.3.17-101.1  
php53-gmp-5.3.17-101.1  
php53-zip-5.3.17-101.1  
php53-calendar-5.3.17-101.1  
php53-sysvmsg-5.3.17-101.1  
php53-shmop-5.3.17-101.1  
php53-ftp-5.3.17-101.1  
php53-mbstring-5.3.17-101.1  
php53-5.3.17-101.1  
php53-snmp-5.3.17-101.1  
php53-fileinfo-5.3.17-101.1  
php53-intl-5.3.17-101.1  
php53-openssl-5.3.17-101.1  
php53-exif-5.3.17-101.1  
php53-pear-5.3.17-101.1  
php53-suhosin-5.3.17-101.1  
php53-sysvsem-5.3.17-101.1  
php53-xmlwriter-5.3.17-101.1  
php53-mcrypt-5.3.17-101.1  
php53-ctype-5.3.17-101.1  
php53-tokenizer-5.3.17-101.1  
apache2-mod\_php53-5.3.17-101.1

## 145236 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0555-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2616

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0555-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002662.html>

SuSE SLES 12 SP1  
noarch  
util-linux-lang-2.25-40.1

x86\_64  
uuid-2.25-40.1  
util-linux-debuginfo-2.25-40.1  
util-linux-debugsource-2.25-40.1  
libuuid1-32bit-2.25-40.1  
libmount1-2.25-40.1  
python-libmount-debuginfo-2.25-40.2  
libuuid1-debuginfo-2.25-40.1  
libblkid1-2.25-40.1  
libsmartcols1-debuginfo-2.25-40.1  
util-linux-2.25-40.1  
libuuid1-2.25-40.1  
libuuid1-debuginfo-32bit-2.25-40.1  
libblkid1-debuginfo-32bit-2.25-40.1  
libmount1-debuginfo-2.25-40.1  
libblkid1-32bit-2.25-40.1  
libmount1-32bit-2.25-40.1  
libsmartcols1-2.25-40.1  
util-linux-systemd-2.25-40.1  
libmount1-debuginfo-32bit-2.25-40.1  
uuid-debuginfo-2.25-40.1  
python-libmount-2.25-40.2  
util-linux-systemd-debuginfo-2.25-40.1  
util-linux-systemd-debugsource-2.25-40.1  
libblkid1-debuginfo-2.25-40.1  
python-libmount-debugsource-2.25-40.2

#### SuSE SLED 12 SP1

x86\_64  
uuid-2.25-40.1  
util-linux-debuginfo-2.25-40.1  
python-libmount-debuginfo-2.25-40.2  
libuuid1-32bit-2.25-40.1  
libmount1-2.25-40.1  
libblkid1-debuginfo-32bit-2.25-40.1  
util-linux-debugsource-2.25-40.1  
libblkid1-2.25-40.1  
libmount1-32bit-2.25-40.1  
util-linux-2.25-40.1  
libuuid1-2.25-40.1  
python-libmount-debugsource-2.25-40.2  
libuuid1-debuginfo-32bit-2.25-40.1  
libuuid1-debuginfo-2.25-40.1  
libmount1-debuginfo-2.25-40.1  
libblkid1-debuginfo-2.25-40.1  
libblkid1-32bit-2.25-40.1  
libsmartcols1-2.25-40.1  
util-linux-systemd-2.25-40.1  
libmount1-debuginfo-32bit-2.25-40.1  
uuid-debuginfo-2.25-40.1  
python-libmount-2.25-40.2  
util-linux-systemd-debuginfo-2.25-40.1  
util-linux-systemd-debugsource-2.25-40.1  
libuuid-devel-2.25-40.1  
libsmartcols1-debuginfo-2.25-40.1

#### noarch

util-linux-lang-2.25-40.1



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

Risk Level: High

CVE: CVE-2017-2616

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0554-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002661.html>

### SuSE SLED 12 SP2

x86\_64

libuuid1-32bit-2.28-44.3.1

util-linux-2.28-44.3.1

libuuid1-debuginfo-2.28-44.3.1

python-libmount-2.28-44.3.3

libblkid1-debuginfo-32bit-2.28-44.3.1

util-linux-systemd-2.28-44.3.3

util-linux-debugsource-2.28-44.3.1

libblkid1-32bit-2.28-44.3.1

uuid-debuginfo-2.28-44.3.3

libmount1-debuginfo-2.28-44.3.1

libmount1-2.28-44.3.1

util-linux-systemd-debugsource-2.28-44.3.3

python-libmount-debugsource-2.28-44.3.3

libsmartcols1-2.28-44.3.1

libuuid-devel-2.28-44.3.1

libuuid1-2.28-44.3.1

util-linux-debuginfo-2.28-44.3.1

libfdisk1-debuginfo-2.28-44.3.1

libblkid1-2.28-44.3.1

libfdisk1-2.28-44.3.1

libuuid1-debuginfo-32bit-2.28-44.3.1

libmount1-debuginfo-32bit-2.28-44.3.1

python-libmount-debuginfo-2.28-44.3.3

libblkid1-debuginfo-2.28-44.3.1

libmount1-32bit-2.28-44.3.1

uuid-2.28-44.3.3

util-linux-systemd-debuginfo-2.28-44.3.3

libsmartcols1-debuginfo-2.28-44.3.1

noarch

util-linux-lang-2.28-44.3.1

### SuSE SLES 12 SP2

noarch

util-linux-lang-2.28-44.3.1

x86\_64

uuid-debuginfo-2.28-44.3.3

util-linux-2.28-44.3.1

libuuid1-debuginfo-2.28-44.3.1

python-libmount-2.28-44.3.3

libuuid1-32bit-2.28-44.3.1  
libblkid1-debuginfo-32bit-2.28-44.3.1  
util-linux-systemd-2.28-44.3.3  
util-linux-debugsource-2.28-44.3.1  
libblkid1-32bit-2.28-44.3.1  
libmount1-debuginfo-2.28-44.3.1  
libmount1-2.28-44.3.1  
util-linux-systemd-debugsource-2.28-44.3.3  
python-libmount-debugsource-2.28-44.3.3  
libsmartcols1-2.28-44.3.1  
libuuid1-2.28-44.3.1  
util-linux-debuginfo-2.28-44.3.1  
libfdisk1-debuginfo-2.28-44.3.1  
libblkid1-2.28-44.3.1  
libfdisk1-2.28-44.3.1  
libuuid1-debuginfo-32bit-2.28-44.3.1  
libmount1-debuginfo-32bit-2.28-44.3.1  
python-libmount-debuginfo-2.28-44.3.3  
libblkid1-debuginfo-2.28-44.3.1  
libmount1-32bit-2.28-44.3.1  
uuuid-2.28-44.3.3  
util-linux-systemd-debuginfo-2.28-44.3.3  
libsmartcols1-debuginfo-2.28-44.3.1

## 185591 - Ubuntu Linux 16.04, 16.10 USN-3211-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10162, CVE-2016-7479, CVE-2016-9137, CVE-2016-9935, CVE-2016-9936, CVE-2017-5340

### Description

The scan detected that the host is missing the following update:  
USN-3211-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003748.html>

Ubuntu 16.10

php7.0-cgi\_7.0.15-0ubuntu0.16.10.2  
php7.0-fpm\_7.0.15-0ubuntu0.16.10.2  
libapache2-mod-php7.0\_7.0.15-0ubuntu0.16.10.2  
php7.0-cli\_7.0.15-0ubuntu0.16.10.2

Ubuntu 16.04

php7.0-cgi\_7.0.15-0ubuntu0.16.04.2  
php7.0-fpm\_7.0.15-0ubuntu0.16.04.2  
libapache2-mod-php7.0\_7.0.15-0ubuntu0.16.04.2  
php7.0-cli\_7.0.15-0ubuntu0.16.04.2

## 185592 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3212-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7554, CVE-2015-8668, CVE-2016-10092, CVE-2016-10093, CVE-2016-10094, CVE-2016-3622, CVE-2016-3623, CVE-2016-3624, CVE-2016-3632, CVE-2016-3658, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991, CVE-2016-5314, CVE-2016-5315, CVE-2016-5316, CVE-2016-5317, CVE-2016-5320, CVE-2016-5321, CVE-2016-5322, CVE-2016-5323, CVE-2016-5652, CVE-2016-5875, CVE-2016-6223, CVE-2016-8331, CVE-2016-9273, CVE-2016-9297, CVE-2016-9448, CVE-2016-9453, CVE-2016-9532, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9538, CVE-2016-9539, CVE-2016-9540, CVE-2017-5225

#### Description

The scan detected that the host is missing the following update:  
USN-3212-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003750.html>

Ubuntu 16.04

libtiff-tools\_4.0.6-1ubuntu0.1  
libtiff5\_4.0.6-1ubuntu0.1

Ubuntu 14.04

libtiff5\_4.0.3-7ubuntu0.6  
libtiff-tools\_4.0.3-7ubuntu0.6

Ubuntu 16.10

libtiff5\_4.0.6-2ubuntu0.1  
libtiff-tools\_4.0.6-2ubuntu0.1

### 185593 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3213-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10166, CVE-2016-10167, CVE-2016-10168, CVE-2016-6906, CVE-2016-6912, CVE-2016-9317, CVE-2016-9933

#### Description

The scan detected that the host is missing the following update:  
USN-3213-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003751.html>

Ubuntu 12.04

libgd2-noxpm\_2.0.36~rc1~dfsg-6ubuntu2.4  
libgd2-xpm\_2.0.36~rc1~dfsg-6ubuntu2.4

Ubuntu 16.04

libgd3\_2.1.1-4ubuntu0.16.04.6

Ubuntu 14.04

libgd3\_2.1.0-3ubuntu0.6

Ubuntu 16.10

libgd3\_2.2.1-1ubuntu3.3

### 191750 - Fedora Linux 24 FEDORA-2017-9b2cf468d5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5953

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-9b2cf468d5

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=1>

Fedora Core 24

vim-8.0.324-1.fc24

### 191765 - Fedora Linux 25 FEDORA-2017-dc6023e849 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10132, CVE-2016-10133, CVE-2016-10141, CVE-2017-5627, CVE-2017-5628

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-dc6023e849

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=4>

Fedora Core 25

mujs-0-8.20170124git4006739.fc25

### 191767 - Fedora Linux 24 FEDORA-2017-624e2eeda0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10132, CVE-2016-10133, CVE-2016-10141, CVE-2017-5627, CVE-2017-5628

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-624e2eeda0

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=3>

Fedora Core 24

mujs-0-8.20170124git4006739.fc24

## **191778 - Fedora Linux 24 FEDORA-2017-ba9c6a3634 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-5495

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-ba9c6a3634

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 24

quagga-0.99.24.1-5.fc24

## **141431 - Red Hat Enterprise Linux RHSA-2017-0336 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0336

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0336.html>

RHEL7S

ppc64

java-1.7.1-ibm-1.7.1.4.1-1jpp.2.el7

java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.2.el7

## RHEL6S

i386

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

x86\_64

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

## RHEL6WS

x86\_64

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

i386

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

## RHEL7D

x86\_64

java-1.7.1-ibm-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.2.el7

## RHEL6D

x86\_64

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

i386

java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.1.el6\_8

java-1.7.1-ibm-src-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.1.el6\_8  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.1.el6\_8

RHEL7WS

x86\_64

java-1.7.1-ibm-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-jdbc-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-demo-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-src-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-devel-1.7.1.4.1-1jpp.2.el7  
java-1.7.1-ibm-plugin-1.7.1.4.1-1jpp.2.el7

## 141433 - Red Hat Enterprise Linux RHSA-2017-0337 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5547, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272, CVE-2017-3289

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0337

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0337.html>

RHEL5D

x86\_64

java-1.7.0-ibm-plugin-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-jdbc-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-demo-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-devel-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-src-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-1.7.0.10.1-1jpp.1.el5\_11

i386

java-1.7.0-ibm-plugin-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-jdbc-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-demo-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-devel-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-src-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-1.7.0.10.1-1jpp.1.el5\_11

RHEL5S

i386

java-1.7.0-ibm-plugin-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-jdbc-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-demo-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-devel-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-src-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-1.7.0.10.1-1jpp.1.el5\_11

x86\_64  
java-1.7.0-ibm-plugin-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-jdbc-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-demo-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-devel-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-src-1.7.0.10.1-1jpp.1.el5\_11  
java-1.7.0-ibm-1.7.0.10.1-1jpp.1.el5\_11

## 141435 - Red Hat Enterprise Linux RHSA-2017-0338 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183, CVE-2016-5546, CVE-2016-5548, CVE-2016-5549, CVE-2016-5552, CVE-2017-3231, CVE-2017-3241, CVE-2017-3252, CVE-2017-3253, CVE-2017-3259, CVE-2017-3261, CVE-2017-3272

### Description

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

RHSA-2017-0338

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0338.html>

### RHEL5S

i386  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-accessibility-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el5\_11

### x86\_64

java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-accessibility-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el5\_11

### RHEL6D

x86\_64  
java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

### i386

java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8



java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

#### RHEL6S

i386

java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

x86\_64

java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

#### RHEL6WS

x86\_64

java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

i386

java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el6\_8  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el6\_8

#### RHEL5D

x86\_64

java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-accessibility-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el5\_11

i386

java-1.6.0-ibm-javacomm-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-demo-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-1.6.0.16.41-1jpp.1.el5\_11

java-1.6.0-ibm-src-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-plugin-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-accessibility-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-devel-1.6.0.16.41-1jpp.1.el5\_11  
java-1.6.0-ibm-jdbc-1.6.0.16.41-1jpp.1.el5\_11

### 182292 - FreeBSD potrace Multiple Memory Failure (f4eb9a25-fde0-11e6-9ad0-b8aeed92ecc4)

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

Risk Level: Medium

CVE: CVE-2016-8685, CVE-2016-8686

#### Description

The scan detected that the host is missing the following update:  
potrace -- multiple memory failure (f4eb9a25-fde0-11e6-9ad0-b8aeed92ecc4)

#### Observation

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

<http://www.vuxml.org/freebsd/f4eb9a25-fde0-11e6-9ad0-b8aeed92ecc4.html>

Affected packages:

potrace < 1.13

### 191764 - Fedora Linux 24 FEDORA-2017-b1abcbe695 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-b1abcbe695

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 24

webkitgtk4-2.14.5-1.fc24

### 191775 - Fedora Linux 25 FEDORA-2017-0beb752b6e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2350, CVE-2017-2354, CVE-2017-2355, CVE-2017-2356, CVE-2017-2362, CVE-2017-2363, CVE-2017-2364, CVE-2017-2365, CVE-2017-2366, CVE-2017-2369, CVE-2017-2371, CVE-2017-2373

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-0beb752b6e

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 25

webkitgtk4-2.14.5-1.fc25

### **21298 - (K61045143) F5 BIG-IP Configuration Utility CSRF Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Description

A vulnerability is present in some versions of F5 BIG-IP systems.

#### Observation

F5's BIG-IP products are network appliances that run F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Traffic Management User Interface (TMUI). Successful exploitation could allow an attacker to launch cross-site request forgery (CSRF) attacks.

### **21309 - (K59298921) F5 BIG-IP OpenSSL Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2181

#### Description

A denial of service vulnerability is present in some versions of F5 BIG-IP products.

#### 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 products. The flaw lies in the OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition.

### **130707 - Debian Linux 8.0 DSA-3797-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-8674, CVE-2017-5896, CVE-2017-5991

#### Description

The scan detected that the host is missing the following update:  
DSA-3797-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3797>

Debian 8.0  
all  
mupdf\_1.5-1+deb8u2

### **178411 - Gentoo Linux GLSA-201702-32 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10173

### Description

The scan detected that the host is missing the following update:  
GLSA-201702-32

### Observation

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

<https://security.gentoo.org/glsa/201702-32>

Affected packages:  
dev-ruby/archive-tar-minitar < 0.6.1

### **178412 - Gentoo Linux GLSA-201702-31 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7976, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8602

### Description

The scan detected that the host is missing the following update:  
GLSA-201702-31

### Observation

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

<https://security.gentoo.org/glsa/201702-31>

Affected packages:  
app-text/ghostscript-gpl < 9.20-r1

### **191753 - Fedora Linux 25 FEDORA-2017-8fffbae8af Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2013-1430

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-8fffbae8af

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 25

xrdp-0.9.1-5.fc25

## **21288 - IBM Tivoli Storage Manager for Virtual Environments Password Disclosure Vulnerability (swg21995544)**

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

Risk Level: Medium

CVE: CVE-2016-6034

### Description

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments.

### Observation

IBM Tivoli Storage Manager for Virtual Environments is a software solution for administrative tasks of storage instances in virtualization environments.

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments. The flaw lies in the component known as Data Protection for VMware GUI. Successful exploitation could allow a highly privileged user logged in to the system to obtain the Windows Domain credentials.

## **130705 - Debian Linux 8.0 DSA-3793-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6252, CVE-2017-2616

### Description

The scan detected that the host is missing the following update:  
DSA-3793-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3793>

Debian 8.0

all

uidmap\_1:4.2-3+deb8u3

login\_1:4.2-3+deb8u3

passwd\_1:4.2-3+deb8u3

## 191751 - Fedora Linux 25 FEDORA-2017-3fb57530fb Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5593

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-3fb57530fb

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=3>

Fedora Core 25

kopete-16.12.2-2.fc25

## 191752 - Fedora Linux 24 FEDORA-2017-844445f2aa Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6265

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-844445f2aa

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

mupdf-1.10a-1.fc24

## 191763 - Fedora Linux 25 FEDORA-2017-6fe982684d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6265

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-6fe982684d

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

mupdf-1.10a-1.fc25

### 191768 - Fedora Linux 24 FEDORA-2017-40d29c8e84 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5593

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-40d29c8e84

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 24

kopete-16.12.2-2.fc24

### 130706 - Debian Linux 8.0 DSA-3796-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-8743

#### Description

The scan detected that the host is missing the following update:  
DSA-3796-1

#### Observation

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

<http://www.debian.org/security/2017/dsa-3796>

Debian 8.0

all

apache2\_2.4.10-10+deb8u8

### 130709 - Debian Linux 8.0 DSA-3795-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-3135

#### Description

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

DSA-3795-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3795>

Debian 8.0

all

bind9\_1:9.9.5.dfsg-9+deb8u10

### **130710 - Debian Linux 8.0 DSA-3792-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2017-3157

### Description

The scan detected that the host is missing the following update:  
DSA-3792-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3792>

Debian 8.0

all

libreoffice\_1:4.3.3-2+deb8u6

### **141430 - Red Hat Enterprise Linux RHSA-2017-0340 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-0340

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2017-0340.html>

RHEL5D

x86\_64

redhat-release-5Client-5.11.0.8

i386

redhat-release-5Client-5.11.0.8



RHEL5S  
i386  
redhat-release-5Server-5.11.0.8

x86\_64  
redhat-release-5Server-5.11.0.8

### 141437 - Red Hat Enterprise Linux RHSA-2017-0339 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

RHSA-2017-0339

#### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0339.html>

RHEL4ES  
x86\_64  
redhat-release-4ES-10.15

i386  
redhat-release-4ES-10.15

RHEL4AS  
i386  
redhat-release-4AS-10.15

x86\_64  
redhat-release-4AS-10.15

### 182291 - FreeBSD xen-tools Cirrus\_bitblt\_cputovideo Does Not Check If Memory Region Is Safe (8cbd9c08-f8b9-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2017-2620

#### Description

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

xen-tools -- cirrus\_bitblt\_cputovideo does not check if memory region is safe (8cbd9c08-f8b9-11e6-ae1b-002590263bf5)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/8cbd9c08-f8b9-11e6-ae1b-002590263bf5.html>

Affected packages:

xen-tools < 4.7.1\_4

## 182293 - FreeBSD MPD Buffer Overflows In Http Output (765d165b-fbfe-11e6-aae7-5404a68ad561)

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:

MPD -- buffer overflows in http output (765d165b-fbfe-11e6-aae7-5404a68ad561)

### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/765d165b-fbfe-11e6-aae7-5404a68ad561.html>

Affected packages:

musicpd < 0.20.5

## 182294 - FreeBSD cURL OcsP Status Validation Error (311e4b1c-f8ee-11e6-9940-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2017-2629

### Description

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

cURL -- ocsP status validation error (311e4b1c-f8ee-11e6-9940-b499baebfeaf)

### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/311e4b1c-f8ee-11e6-9940-b499baebfeaf.html>

Affected packages:

7.52.0 <= curl < 7.53.0

## 185594 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3142-2 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-3142-2

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-February/003747.html>

Ubuntu 12.04

libmagickcore4\_6.6.9.7-5ubuntu3.7  
libmagickcore4-extra\_6.6.9.7-5ubuntu3.7  
imagemagick\_6.6.9.7-5ubuntu3.7

Ubuntu 16.04

imagemagick\_6.8.9.9-7ubuntu5.4  
libmagickcore-6.q16-2\_6.8.9.9-7ubuntu5.4  
libmagickcore-6.q16-2-extra\_6.8.9.9-7ubuntu5.4  
imagemagick-6.q16\_6.8.9.9-7ubuntu5.4

Ubuntu 14.04

libmagickcore5\_6.7.7.10-6ubuntu3.4  
libmagickcore5-extra\_6.7.7.10-6ubuntu3.4  
imagemagick\_6.7.7.10-6ubuntu3.4

Ubuntu 16.10

imagemagick\_6.8.9.9-7ubuntu8.3  
libmagickcore-6.q16-2-extra\_6.8.9.9-7ubuntu8.3  
libmagickcore-6.q16-2\_6.8.9.9-7ubuntu8.3  
imagemagick-6.q16\_6.8.9.9-7ubuntu8.3

#### **191754 - Fedora Linux 25 FEDORA-2017-beb25f1953 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-2017-beb25f1953

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

rpm-4.13.0.1-1.fc25

#### **191756 - Fedora Linux 25 FEDORA-2017-376ae2b92c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8745

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-376ae2b92c

### Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=4>

Fedora Core 25

tomcat-8.0.41-1.fc25

### **191757 - Fedora Linux 24 FEDORA-2017-a8dc348834 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2017-6004

### Description

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

FEDORA-2017-a8dc348834

### Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=3>

Fedora Core 24

pcre-8.40-2.fc24

### **191758 - Fedora Linux 24 FEDORA-2017-19c5440abe Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8745

### Description

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

FEDORA-2017-19c5440abe

### Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

tomcat-8.0.41-1.fc24

### **191759 - Fedora Linux 25 FEDORA-2017-c1cd67adc1 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-2017-c1cd67adc1

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=4>

Fedora Core 25

plasma-desktop-5.8.5-4.fc25

### **191760 - Fedora Linux 25 FEDORA-2017-2b0459f416 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-2017-2b0459f416

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 25

python-PyMySQL-0.7.10-10.fc25

### **191762 - Fedora Linux 25 FEDORA-2017-0fbbb732a3 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-2017-0fbbb732a3

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=1>

Fedora Core 25

firebird-2.5.7.27050.0-1.fc25

## 191766 - Fedora Linux 24 FEDORA-2017-13b5cb36c3 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-2017-13b5cb36c3

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=3>

Fedora Core 24

plasma-desktop-5.8.5-4.fc24

## 191769 - Fedora Linux 25 FEDORA-2017-101722eb25 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-0359

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-101722eb25

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=4>

Fedora Core 25

diffoscope-77-1.fc25

## 191770 - Fedora Linux 24 FEDORA-2017-33cb46c6b0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-0359

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-33cb46c6b0

### Observation

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

For more information see:

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=3>

Fedora Core 24

diffoscope-77-1.fc24

### 191771 - Fedora Linux 24 FEDORA-2017-b11b460865 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2616

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-b11b460865

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 24

util-linux-2.28.2-2.fc24

### 191772 - Fedora Linux 25 FEDORA-2017-20710607f5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2616

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-20710607f5

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 25

util-linux-2.28.2-2.fc25

### 191773 - Fedora Linux 25 FEDORA-2017-266ab882cd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2620

## Description

The scan detected that the host is missing the following update:  
FEDORA-2017-266ab882cd

## Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/3/?count=200&page=1>

Fedora Core 25

xen-4.7.1-9.fc25

### **191774 - Fedora Linux 25 FEDORA-2017-7803508155 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-2017-7803508155

## Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 25

python-cjson-1.1.0-9.fc25

### **191776 - Fedora Linux 24 FEDORA-2017-abbfa3f1a9 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-2017-abbfa3f1a9

## Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 24

python-cjson-1.1.0-9.fc24



## 21290 - IBM Tivoli Storage Manager for Virtual Environments vCenter Password Disclosure Vulnerability (swg21996198)

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

Risk Level: Low

CVE: CVE-2016-6110

### Description

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments.

### Observation

IBM Tivoli Storage Manager for Virtual Environments is a software solution for administrative tasks of storage instances in virtualization environments.

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments. The flaw is due to an issue in the VM backup subsystem. Successful exploitation could allow an authenticated user to obtain the vCenter password.

## 21291 - IBM Tivoli Storage Manager for Virtual Environments vCenter Password Disclosure Vulnerability (swg21996198)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2016-6110

### Description

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments.

### Observation

IBM Tivoli Storage Manager for Virtual Environments is a software solution for administrative tasks of storage instances in virtualization environments.

An information disclosure vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments. The flaw is due to an issue in the VM backup subsystem. Successful exploitation could allow an authenticated user to obtain the vCenter password.

## 132341 - Oracle VM OVMSA-2017-0043 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2857, CVE-2017-2615

### Description

The scan detected that the host is missing the following update:  
OVMSA-2017-0043

### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-February/000652.html>

OVM3.4

x86\_64

qemu-img-0.12.1.2-2.491.el6\_8.6

## 141436 - Red Hat Enterprise Linux RHSA-2017-0309 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2857, CVE-2017-2615

### Description

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

RHSA-2017-0309

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2017-0309.html>

#### RHEL6D

x86\_64

qemu-kvm-0.12.1.2-2.491.el6\_8.6

qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

qemu-img-0.12.1.2-2.491.el6\_8.6

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

i386

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

#### RHEL6S

i386

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

x86\_64

qemu-kvm-0.12.1.2-2.491.el6\_8.6

qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

qemu-img-0.12.1.2-2.491.el6\_8.6

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

#### RHEL6WS

x86\_64

qemu-kvm-0.12.1.2-2.491.el6\_8.6

qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

qemu-img-0.12.1.2-2.491.el6\_8.6

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

i386

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

## 145235 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0571-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0571-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002667.html>

SuSE SLED 12 SP2

x86\_64

xen-libs-32bit-4.7.1\_06-31.1

xen-4.7.1\_06-31.1

xen-libs-debuginfo-32bit-4.7.1\_06-31.1

xen-libs-4.7.1\_06-31.1

xen-debugsource-4.7.1\_06-31.1

xen-libs-debuginfo-4.7.1\_06-31.1

SuSE SLES 12 SP2

x86\_64

xen-libs-32bit-4.7.1\_06-31.1

xen-doc-html-4.7.1\_06-31.1

xen-tools-4.7.1\_06-31.1

xen-4.7.1\_06-31.1

xen-tools-domU-4.7.1\_06-31.1

xen-libs-debuginfo-32bit-4.7.1\_06-31.1

xen-libs-4.7.1\_06-31.1

xen-tools-domU-debuginfo-4.7.1\_06-31.1

xen-debugsource-4.7.1\_06-31.1

xen-libs-debuginfo-4.7.1\_06-31.1

xen-tools-debuginfo-4.7.1\_06-31.1

## **145238 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0570-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-10155, CVE-2016-9101, CVE-2016-9776, CVE-2016-9907, CVE-2016-9911, CVE-2016-9921, CVE-2016-9922, CVE-2017-2615, CVE-2017-2620, CVE-2017-5579, CVE-2017-5856, CVE-2017-5898, CVE-2017-5973

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:0570-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-February/002666.html>

SuSE SLES 12 SP1

x86\_64

xen-tools-domU-4.5.5\_06-22.11.2

xen-libs-4.5.5\_06-22.11.2

xen-debugsource-4.5.5\_06-22.11.2

xen-tools-debuginfo-4.5.5\_06-22.11.2

xen-libs-debuginfo-32bit-4.5.5\_06-22.11.2  
xen-tools-4.5.5\_06-22.11.2  
xen-kmp-default-debuginfo-4.5.5\_06\_k3.12.69\_60.64.32-22.11.2  
xen-tools-domU-debuginfo-4.5.5\_06-22.11.2  
xen-kmp-default-4.5.5\_06\_k3.12.69\_60.64.32-22.11.2  
xen-libs-32bit-4.5.5\_06-22.11.2  
xen-libs-debuginfo-4.5.5\_06-22.11.2  
xen-doc-html-4.5.5\_06-22.11.2  
xen-4.5.5\_06-22.11.2

SuSE SLED 12 SP1  
x86\_64

xen-libs-debuginfo-4.5.5\_06-22.11.2  
xen-libs-4.5.5\_06-22.11.2  
xen-libs-32bit-4.5.5\_06-22.11.2  
xen-kmp-default-4.5.5\_06\_k3.12.69\_60.64.32-22.11.2  
xen-debugsource-4.5.5\_06-22.11.2  
xen-kmp-default-debuginfo-4.5.5\_06\_k3.12.69\_60.64.32-22.11.2  
xen-libs-debuginfo-32bit-4.5.5\_06-22.11.2  
xen-4.5.5\_06-22.11.2

### 160217 - CentOS 6 CESA-2017-0309 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2857, CVE-2017-2615

#### Description

The scan detected that the host is missing the following update:  
CESA-2017-0309

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-February/022287.html>

CentOS 6  
x86\_64  
qemu-kvm-0.12.1.2-2.491.el6\_8.6  
qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6  
qemu-img-0.12.1.2-2.491.el6\_8.6  
qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

i686  
qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

### 163289 - Oracle Enterprise Linux ELSA-2017-0309 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-2857, CVE-2017-2615

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-0309

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-February/006722.html>

OEL6

x86\_64

qemu-kvm-0.12.1.2-2.491.el6\_8.6

qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6

qemu-img-0.12.1.2-2.491.el6\_8.6

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

i386

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

### **175118 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86\_64 (1702-5279)**

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

Risk Level: Low

CVE: CVE-2016-2857, CVE-2017-2615

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: qemu-kvm on SL6.x i386/x86\_64 (1702-5279)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1702&L=scientific-linux-errata&F=&S=&P=5279>

SL6

x86\_64

qemu-kvm-0.12.1.2-2.491.el6\_8.6

qemu-kvm-tools-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

qemu-img-0.12.1.2-2.491.el6\_8.6

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

i386

qemu-guest-agent-0.12.1.2-2.491.el6\_8.6

qemu-kvm-debuginfo-0.12.1.2-2.491.el6\_8.6

### **191777 - Fedora Linux 24 FEDORA-2017-d4ee7018c1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9776, CVE-2017-2615, CVE-2017-5525, CVE-2017-5526

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-d4ee7018c1

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/2/?count=200&page=2>

Fedora Core 24

xen-4.6.4-7.fc24

### 130704 - Debian Linux 8.0 DSA-3794-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6188

#### Description

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

DSA-3794-1

#### Observation

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

For more information see:

<http://www.debian.org/security/2017/dsa-3794>

Debian 8.0

all

munin\_2.0.25-1+deb8u1

## 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.

### 141413 - Red Hat Enterprise Linux RHSA-2017-0184 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662, CVE-2016-6663

#### Update Details

CVE is updated

### 144975 - SuSE Linux 13.1 openSUSE-SU-2016:2737-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2014-8137, CVE-2014-8138, CVE-2014-8157, CVE-2014-8158, CVE-2014-9029, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

#### Update Details

CVE is updated

### 144983 - SuSE Linux 13.2 openSUSE-SU-2016:2722-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8886

#### Update Details

CVE is updated

### 144989 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2775-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2014-8158, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

#### Update Details

CVE is updated

### 144992 - SuSE SLES 11 SP4 SUSE-SU-2016:2776-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2011-4516, CVE-2011-4517, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

#### Update Details

CVE is updated

### 160204 - CentOS 6 CESA-2017-0184 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662, CVE-2016-6663

#### Update Details

CVE is updated

### 163269 - Oracle Enterprise Linux ELSA-2017-0184 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662, CVE-2016-6663

#### Update Details

CVE is updated

### 175049 - Scientific Linux Security ERRATA Important: mariadb on SL7.x x86\_64 (1612-6698)

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

Update Details

CVE is updated

**175106 - Scientific Linux Security ERRATA Important: mysql on SL6.x i386/x86\_64 (1701-11125)**

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

Risk Level: High

CVE: CVE-2016-6662, CVE-2016-6663

Update Details

CVE is updated

**20924 - IBM Tivoli Storage Manager FastBack Multiple Vulnerabilities (swg21993916)**

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

Risk Level: High

CVE: CVE-2015-0119, CVE-2015-1897

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated CVE is updated

**160203 - CentOS 5, 6, 7 CESA-2017-0190 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-5373, CVE-2017-5375, CVE-2017-5376, CVE-2017-5378, CVE-2017-5380, CVE-2017-5383, CVE-2017-5386, CVE-2017-5390, CVE-2017-5396

Update Details

FASLScript is updated

**145080 - SuSE Linux 13.2 openSUSE-SU-2016:3032-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-4552

Update Details

CVE is updated

**145140 - SuSE Linux 13.1 openSUSE-SU-2016:3309-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-4552



[Update Details](#)

CVE is updated

**178392 - Gentoo Linux GLSA-201702-14 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-7459

[Update Details](#)

Risk is updated

**190943 - Fedora Linux 24 FEDORA-2016-f3b40fcbc3 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-3102

[Update Details](#)

Risk is updated

**191210 - Fedora Linux 25 FEDORA-2016-9960d370f7 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6173

[Update Details](#)

Risk is updated

**191220 - Fedora Linux 24 FEDORA-2016-e1d4972701 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6173

[Update Details](#)

Risk is updated

**191662 - Fedora Linux 25 FEDORA-2017-7c569d396b Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-7459

[Update Details](#)

Risk is updated

**191665 - Fedora Linux 24 FEDORA-2017-08207fe48b Update Is Not Installed**

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

Risk Level: High  
CVE: CVE-2013-7459

[Update Details](#)

Risk is updated

**191722 - Fedora Linux 25 FEDORA-2017-fb89ca752a Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-5897, CVE-2017-5986

[Update Details](#)

Risk is updated

**145143 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0084-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-8654, CVE-2016-9395, CVE-2016-9398, CVE-2016-9560, CVE-2016-9591

[Update Details](#)

Risk is updated

**182258 - FreeBSD MySQL Multiple Vulnerabilities (22373c43-d728-11e6-a9a5-b499baebfeaf)**

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

[Update Details](#)

CVE is updated

**191535 - Fedora Linux 24 FEDORA-2016-c7e60a9fd4 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5609, CVE-2016-5612, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

[Update Details](#)

CVE is updated

**191547 - Fedora Linux 25 FEDORA-2016-9b83c6862d Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5609, CVE-2016-5612, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

[Update Details](#)

CVE is updated

### **20601 - (SYM16-015) Symantec Endpoint Protection Decomposer Engine Multiple Vulnerabilities**

Category: Windows Host Assessment -> Anti-Virus Software  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-5309, CVE-2016-5310

#### Update Details

FASLScript is updated

### **21272 - Hanwha Techwin Smart Security Manager Multiple Vulnerabilities**

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

Risk Level: Medium

CVE: CVE-2017-5168, CVE-2017-5169

#### Update Details

Risk is updated

### **88836 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-365-01 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10087

#### Update Details

Risk is updated

### **130649 - Debian Linux 8.0 DSA-3742-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9956

#### Update Details

Risk is updated

### **130657 - Debian Linux 8.0 DSA-3745-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10002

#### Update Details

Risk is updated

### **130662 - Debian Linux 8.0 DSA-3749-1 Update Is Not Installed**

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

Risk Level: Medium  
CVE: CVE-2015-8979

[Update Details](#)

Risk is updated

**130668 - Debian Linux 8.0 DSA-3752-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-10109

[Update Details](#)

Risk is updated

**130676 - Debian Linux 8.0 DSA-3760-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-10026, CVE-2016-9646, CVE-2017-0356

[Update Details](#)

Risk is updated

**130690 - Debian Linux 8.0 DSA-3778-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-10173

[Update Details](#)

Risk is updated

**145173 - SuSE Linux 13.2 openSUSE-SU-2017:0178-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-10109

[Update Details](#)

Risk is updated

**145193 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0286-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-10109

[Update Details](#)

Risk is updated

### **175075 - Scientific Linux Security ERRATA Moderate: ntp on SL7.x x86\_64 (1612-12188)**

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8158

#### Update Details

CVE is updated

### **182234 - FreeBSD squid Multiple Vulnerabilities (41f8af15-c8b9-11e6-ae1b-002590263bf5)**

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

Risk Level: Medium

CVE: CVE-2016-10002, CVE-2016-10003

#### Update Details

Risk is updated

### **182254 - FreeBSD Use-After-Free Vulnerability In Pcsc-lite (c218873d-d444-11e6-84ef-f0def167eeea)**

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

Risk Level: Medium

CVE: CVE-2016-10109

#### Update Details

Risk is updated

### **185552 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3176-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10109

#### Update Details

Risk is updated

### **185564 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3192-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10002, CVE-2016-10003

#### Update Details

Risk is updated

### **191580 - Fedora Linux 24 FEDORA-2016-a1f774c3d7 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9956

[Update Details](#)

Risk is updated

**191585 - Fedora Linux 25 FEDORA-2016-01eba63bcc Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9956

[Update Details](#)

Risk is updated

**191589 - Fedora Linux 25 FEDORA-2016-a4b06a036b Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10087

[Update Details](#)

Risk is updated

**191595 - Fedora Linux 24 FEDORA-2016-1a7e14d084 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10087

[Update Details](#)

Risk is updated

**191598 - Fedora Linux 25 FEDORA-2017-1a7b8c0730 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10109

[Update Details](#)

Risk is updated

**191622 - Fedora Linux 24 FEDORA-2017-8311440c55 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10109

[Update Details](#)

Risk is updated

**191645 - Fedora Linux 25 FEDORA-2016-c614315d29 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10002, CVE-2016-10003

[Update Details](#)

Risk is updated

#### **191670 - Fedora Linux 24 FEDORA-2017-8873ebdb43 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10026, CVE-2016-9646, CVE-2017-0356

[Update Details](#)

Risk is updated

#### **191674 - Fedora Linux 25 FEDORA-2017-c756d37779 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-10026, CVE-2016-9646, CVE-2017-0356

[Update Details](#)

Risk is updated

#### **145066 - SuSE Linux 13.2 openSUSE-SU-2016:3027-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9556, CVE-2016-9559

[Update Details](#)

Risk is updated

#### **145067 - SuSE Linux 13.2 openSUSE-SU-2016:3026-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9556, CVE-2016-9559

[Update Details](#)

Risk is updated

#### **170724 - Amazon Linux AMI ALAS-2016-750 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6329

[Update Details](#)

Risk is updated

### **178230 - Gentoo Linux GLSA-201611-02 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6329

#### Update Details

Risk is updated

### **182084 - FreeBSD puppet-agent MCollective plugin Remote Code Execution Vulnerability (df502a2f-61f6-11e6-a461-643150d3111d)**

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

Risk Level: Medium

CVE: CVE-2015-7331

#### Update Details

Risk is updated

### **190337 - Fedora Linux 23 FEDORA-2016-65b7608d8b Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-2402

#### Update Details

Risk is updated

### **191033 - Fedora Linux 24 FEDORA-2016-7810e24465 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6329

#### Update Details

Risk is updated

### **191034 - Fedora Linux 25 FEDORA-2016-81d6e6a9ac Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6329

#### Update Details

Risk is updated

### **191061 - Fedora Linux 23 FEDORA-2016-dc2cb4ad6b Update Is Not Installed**

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

Risk Level: Medium



CVE: CVE-2016-6329

[Update Details](#)

Risk is updated

**191345 - Fedora Linux 23 FEDORA-2016-6c789ba91d Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2011-4516, CVE-2011-4517, CVE-2016-2089, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

[Update Details](#)

CVE is updated

**191351 - Fedora Linux 24 FEDORA-2016-e0f0d48142 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2011-4516, CVE-2011-4517, CVE-2016-2089, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

[Update Details](#)

CVE is updated

**132309 - Oracle VM OVMSA-2016-0171 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9637

[Update Details](#)

Risk is updated

**132311 - Oracle VM OVMSA-2016-0172 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9637

[Update Details](#)

Risk is updated

**141382 - Red Hat Enterprise Linux RHSA-2016-2963 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9637

[Update Details](#)

Risk is updated

### **160180 - CentOS 5 CESA-2016-2963 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9637

#### Update Details

Risk is updated

### **163246 - Oracle Enterprise Linux ELSA-2016-2963 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9637

#### Update Details

Risk is updated

### **175067 - Scientific Linux Security ERRATA Important: xen on SL5.x i386/x86\_64 (1612-17477)**

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

Risk Level: Low

CVE: CVE-2016-9637

#### Update Details

Risk is updated

### **181972 - FreeBSD roundcube XSS Vulnerability (97e86d10-2ea7-11e6-ae88-002590263bf5)**

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

Risk Level: Low

CVE: CVE-2016-4552

#### Update Details

CVE is updated

### **182165 - FreeBSD FreeBSD OpenSSL Remote DoS Vulnerability (0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8)**

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

Risk Level: Low

CVE: CVE-2016-8610

#### Update Details

FASLScript is updated

### **182273 - FreeBSD OpenSSL Multiple Vulnerabilities (d455708a-e3d3-11e6-9940-b499baebfeaf)**

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

Risk Level: Low

CVE: CVE-2016-7055, CVE-2017-3730, CVE-2017-3731, CVE-2017-3732

[Update Details](#)

FASLScript is updated

**190633 - Fedora Linux 24 FEDORA-2016-d23d2712de Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-4552

[Update Details](#)

CVE is updated

**190772 - Fedora Linux 23 FEDORA-2016-396403ec02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-4552

[Update Details](#)

CVE is updated

**190796 - Fedora Linux 22 FEDORA-2016-e4c559515c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-4552

[Update Details](#)

CVE is updated

**182205 - FreeBSD xen-kernel Guest 32-bit ELF Symbol Table Load Leaking Host Data (5555120d-ba4d-11e6-ae1b-002590263bf5)**

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

Risk Level: Low

CVE: CVE-2016-9384

[Update Details](#)

Risk is updated

## HOW TO UPDATE

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

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

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will

be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

## **MCAFFEE TECHNICAL SUPPORT**

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

Multi-National Phone Support available here:

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

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

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

Copyright 2017 McAfee, Inc.

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