

## 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

#### 132310 - Oracle VM OVMSA-2016-0175 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9555

#### Description

The scan detected that the host is missing the following update:  
OVMSA-2016-0175

#### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000602.html>

OVM3.3  
x86\_64  
kernel-uek-firmware-3.8.13-118.15.1.el6uek  
kernel-uek-3.8.13-118.15.1.el6uek

#### 132314 - Oracle VM OVMSA-2016-0174 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9555

#### Description

The scan detected that the host is missing the following update:  
OVMSA-2016-0174

#### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000601.html>

OVM3.4  
x86\_64  
kernel-uek-4.1.12-61.1.22.el6uek  
kernel-uek-firmware-4.1.12-61.1.22.el6uek

#### 141379 - Red Hat Enterprise Linux RHSA-2016-2928 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2928

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2928.html>

### RHEL6S

x86\_64

rh-mariadb101-mariadb-oqgraph-engine-10.1.19-6.el6  
rh-mariadb101-mariadb-config-10.1.19-6.el6  
rh-mariadb101-mariadb-errmsg-10.1.19-6.el6  
rh-mariadb101-mariadb-server-10.1.19-6.el6  
rh-mariadb101-mariadb-server-galera-10.1.19-6.el6  
rh-mariadb101-mariadb-10.1.19-6.el6  
rh-mariadb101-mariadb-common-10.1.19-6.el6  
rh-mariadb101-mariadb-bench-10.1.19-6.el6  
rh-mariadb101-mariadb-debuginfo-10.1.19-6.el6  
rh-mariadb101-mariadb-devel-10.1.19-6.el6  
rh-mariadb101-mariadb-test-10.1.19-6.el6

### RHEL6WS

x86\_64

rh-mariadb101-mariadb-oqgraph-engine-10.1.19-6.el6  
rh-mariadb101-mariadb-config-10.1.19-6.el6  
rh-mariadb101-mariadb-errmsg-10.1.19-6.el6  
rh-mariadb101-mariadb-server-10.1.19-6.el6  
rh-mariadb101-mariadb-server-galera-10.1.19-6.el6  
rh-mariadb101-mariadb-10.1.19-6.el6  
rh-mariadb101-mariadb-common-10.1.19-6.el6  
rh-mariadb101-mariadb-bench-10.1.19-6.el6  
rh-mariadb101-mariadb-debuginfo-10.1.19-6.el6  
rh-mariadb101-mariadb-devel-10.1.19-6.el6  
rh-mariadb101-mariadb-test-10.1.19-6.el6

### RHEL7S

x86\_64

rh-mariadb101-mariadb-oqgraph-engine-10.1.19-6.el7  
rh-mariadb101-mariadb-test-10.1.19-6.el7  
rh-mariadb101-mariadb-devel-10.1.19-6.el7  
rh-mariadb101-mariadb-server-galera-10.1.19-6.el7  
rh-mariadb101-mariadb-common-10.1.19-6.el7  
rh-mariadb101-mariadb-server-10.1.19-6.el7  
rh-mariadb101-mariadb-10.1.19-6.el7  
rh-mariadb101-mariadb-bench-10.1.19-6.el7  
rh-mariadb101-mariadb-debuginfo-10.1.19-6.el7  
rh-mariadb101-mariadb-config-10.1.19-6.el7  
rh-mariadb101-mariadb-errmsg-10.1.19-6.el7

### RHEL7WS

x86\_64  
rh-mariadb101-mariadb-oqgraph-engine-10.1.19-6.el7  
rh-mariadb101-mariadb-test-10.1.19-6.el7  
rh-mariadb101-mariadb-devel-10.1.19-6.el7  
rh-mariadb101-mariadb-server-galera-10.1.19-6.el7  
rh-mariadb101-mariadb-common-10.1.19-6.el7  
rh-mariadb101-mariadb-server-10.1.19-6.el7  
rh-mariadb101-mariadb-10.1.19-6.el7  
rh-mariadb101-mariadb-bench-10.1.19-6.el7  
rh-mariadb101-mariadb-debuginfo-10.1.19-6.el7  
rh-mariadb101-mariadb-config-10.1.19-6.el7  
rh-mariadb101-mariadb-errmsg-10.1.19-6.el7

## 141380 - Red Hat Enterprise Linux RHSA-2016-2927 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-5630, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2927

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2927.html>

### RHEL6S

x86\_64  
rh-mariadb100-mariadb-bench-10.0.28-5.el6  
rh-mariadb100-mariadb-errmsg-10.0.28-5.el6  
rh-mariadb100-mariadb-config-10.0.28-5.el6  
rh-mariadb100-mariadb-oqgraph-engine-10.0.28-5.el6  
rh-mariadb100-mariadb-devel-10.0.28-5.el6  
rh-mariadb100-mariadb-10.0.28-5.el6  
rh-mariadb100-mariadb-test-10.0.28-5.el6  
rh-mariadb100-mariadb-debuginfo-10.0.28-5.el6  
rh-mariadb100-mariadb-common-10.0.28-5.el6  
rh-mariadb100-mariadb-server-10.0.28-5.el6

### RHEL6WS

x86\_64  
rh-mariadb100-mariadb-bench-10.0.28-5.el6  
rh-mariadb100-mariadb-errmsg-10.0.28-5.el6  
rh-mariadb100-mariadb-config-10.0.28-5.el6  
rh-mariadb100-mariadb-oqgraph-engine-10.0.28-5.el6  
rh-mariadb100-mariadb-devel-10.0.28-5.el6  
rh-mariadb100-mariadb-10.0.28-5.el6  
rh-mariadb100-mariadb-test-10.0.28-5.el6  
rh-mariadb100-mariadb-debuginfo-10.0.28-5.el6  
rh-mariadb100-mariadb-common-10.0.28-5.el6  
rh-mariadb100-mariadb-server-10.0.28-5.el6

### RHEL7S

x86\_64

rh-mariadb100-mariadb-config-10.0.28-5.el7  
rh-mariadb100-mariadb-oqgraph-engine-10.0.28-5.el7  
rh-mariadb100-mariadb-errmsg-10.0.28-5.el7  
rh-mariadb100-mariadb-test-10.0.28-5.el7  
rh-mariadb100-mariadb-server-10.0.28-5.el7  
rh-mariadb100-mariadb-devel-10.0.28-5.el7  
rh-mariadb100-mariadb-bench-10.0.28-5.el7  
rh-mariadb100-mariadb-debuginfo-10.0.28-5.el7  
rh-mariadb100-mariadb-common-10.0.28-5.el7  
rh-mariadb100-mariadb-10.0.28-5.el7

## RHEL7WS

x86\_64

rh-mariadb100-mariadb-config-10.0.28-5.el7  
rh-mariadb100-mariadb-oqgraph-engine-10.0.28-5.el7  
rh-mariadb100-mariadb-errmsg-10.0.28-5.el7  
rh-mariadb100-mariadb-test-10.0.28-5.el7  
rh-mariadb100-mariadb-server-10.0.28-5.el7  
rh-mariadb100-mariadb-devel-10.0.28-5.el7  
rh-mariadb100-mariadb-bench-10.0.28-5.el7  
rh-mariadb100-mariadb-debuginfo-10.0.28-5.el7  
rh-mariadb100-mariadb-common-10.0.28-5.el7  
rh-mariadb100-mariadb-10.0.28-5.el7

## 145056 - SuSE Linux 13.2 openSUSE-SU-2016:3061-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8962, CVE-2015-8963, CVE-2016-7042, CVE-2016-7910, CVE-2016-7911, CVE-2016-7913, CVE-2016-7914, CVE-2016-7916, CVE-2016-8633, CVE-2016-8646, CVE-2016-8655, CVE-2016-9555

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3061-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00058.html>

SuSE Linux 13.2

i586

bbswitch-0.8-3.26.1  
kernel-default-3.16.7-53.1  
ipset-kmp-xen-6.23\_k3.16.7\_53-26.1  
virtualbox-host-kmp-desktop-debuginfo-5.0.30\_k3.16.7\_53-62.1  
pcfclock-debugsource-0.44-260.26.1  
pcfclock-kmp-pae-debuginfo-0.44\_k3.16.7\_53-260.26.1  
xtables-addons-kmp-default-debuginfo-2.6\_k3.16.7\_53-28.1  
virtualbox-5.0.30-62.1  
crash-kmp-default-7.0.8\_k3.16.7\_53-26.1  
xtables-addons-kmp-xen-2.6\_k3.16.7\_53-28.1  
crash-gcore-7.0.8-26.1  
ipset-kmp-default-6.23\_k3.16.7\_53-26.1  
python-virtualbox-5.0.30-62.1  
cloop-kmp-pae-debuginfo-2.639\_k3.16.7\_53-14.26.1  
virtualbox-guest-kmp-default-debuginfo-5.0.30\_k3.16.7\_53-62.1

xen-devel-4.4.4\_05-55.1  
libipset3-debuginfo-6.23-26.1  
vhba-kmp-desktop-20140629\_k3.16.7\_53-2.26.1  
crash-doc-7.0.8-26.1  
kernel-default-devel-3.16.7-53.1  
virtualbox-host-kmp-pae-debuginfo-5.0.30\_k3.16.7\_53-62.1  
virtualbox-websrv-5.0.30-62.1  
bbswitch-debugsource-0.8-3.26.1  
virtualbox-guest-x11-5.0.30-62.1  
cloop-kmp-xen-debuginfo-2.639\_k3.16.7\_53-14.26.1  
kernel-default-debuginfo-3.16.7-53.1  
crash-kmp-xen-7.0.8\_k3.16.7\_53-26.1  
xtables-addons-kmp-default-2.6\_k3.16.7\_53-28.1  
xtables-addons-kmp-pae-debuginfo-2.6\_k3.16.7\_53-28.1  
vhba-kmp-debugsource-20140629-2.26.1  
bbswitch-kmp-default-0.8\_k3.16.7\_53-3.26.1  
hdjmod-debugsource-1.28-18.27.1  
kernel-ec2-base-3.16.7-53.1  
crash-kmp-xen-debuginfo-7.0.8\_k3.16.7\_53-26.1  
hdjmod-kmp-pae-debuginfo-1.28\_k3.16.7\_53-18.27.1  
cloop-kmp-desktop-debuginfo-2.639\_k3.16.7\_53-14.26.1  
ipset-kmp-pae-6.23\_k3.16.7\_53-26.1  
vhba-kmp-default-20140629\_k3.16.7\_53-2.26.1  
cloop-2.639-14.26.1  
kernel-obs-qa-3.16.7-53.1  
hdjmod-kmp-default-1.28\_k3.16.7\_53-18.27.1  
pcfclock-kmp-default-debuginfo-0.44\_k3.16.7\_53-260.26.1  
bbswitch-kmp-pae-0.8\_k3.16.7\_53-3.26.1  
bbswitch-kmp-xen-0.8\_k3.16.7\_53-3.26.1  
ipset-debuginfo-6.23-26.1  
vhba-kmp-xen-debuginfo-20140629\_k3.16.7\_53-2.26.1  
ipset-kmp-desktop-6.23\_k3.16.7\_53-26.1  
kernel-ec2-3.16.7-53.1  
xen-libs-debuginfo-4.4.4\_05-55.1  
xen-tools-domU-debuginfo-4.4.4\_05-55.1  
virtualbox-host-kmp-default-debuginfo-5.0.30\_k3.16.7\_53-62.1  
ipset-kmp-pae-debuginfo-6.23\_k3.16.7\_53-26.1  
pcfclock-kmp-desktop-debuginfo-0.44\_k3.16.7\_53-260.26.1  
virtualbox-host-kmp-pae-5.0.30\_k3.16.7\_53-62.1  
crash-eppic-debuginfo-7.0.8-26.1  
crash-kmp-default-debuginfo-7.0.8\_k3.16.7\_53-26.1  
virtualbox-guest-kmp-pae-5.0.30\_k3.16.7\_53-62.1  
xtables-addons-2.6-28.1  
crash-7.0.8-26.1  
xtables-addons-kmp-pae-2.6\_k3.16.7\_53-28.1  
virtualbox-guest-tools-debuginfo-5.0.30-62.1  
bbswitch-kmp-default-debuginfo-0.8\_k3.16.7\_53-3.26.1  
kernel-syms-3.16.7-53.1  
virtualbox-guest-kmp-desktop-5.0.30\_k3.16.7\_53-62.1  
cloop-kmp-default-2.639\_k3.16.7\_53-14.26.1  
cloop-kmp-xen-2.639\_k3.16.7\_53-14.26.1  
xtables-addons-kmp-desktop-2.6\_k3.16.7\_53-28.1  
xtables-addons-debuginfo-2.6-28.1  
bbswitch-kmp-pae-debuginfo-0.8\_k3.16.7\_53-3.26.1  
ipset-kmp-desktop-debuginfo-6.23\_k3.16.7\_53-26.1  
kernel-default-base-3.16.7-53.1  
pcfclock-debuginfo-0.44-260.26.1  
crash-kmp-desktop-7.0.8\_k3.16.7\_53-26.1  
pcfclock-kmp-desktop-0.44\_k3.16.7\_53-260.26.1  
crash-debugsource-7.0.8-26.1

crash-gcore-debuginfo-7.0.8-26.1  
crash-kmp-desktop-debuginfo-7.0.8\_k3.16.7\_53-26.1  
vhba-kmp-pae-20140629\_k3.16.7\_53-2.26.1  
virtualbox-websrv-debuginfo-5.0.30-62.1  
ipset-devel-6.23-26.1  
vhba-kmp-desktop-debuginfo-20140629\_k3.16.7\_53-2.26.1  
kernel-obs-build-3.16.7-53.2  
virtualbox-guest-tools-5.0.30-62.1  
hdjmod-kmp-desktop-1.28\_k3.16.7\_53-18.27.1  
virtualbox-guest-kmp-pae-debuginfo-5.0.30\_k3.16.7\_53-62.1  
xen-libs-4.4.4\_05-55.1  
ipset-6.23-26.1  
kernel-default-debugsource-3.16.7-53.1  
ipset-kmp-default-debuginfo-6.23\_k3.16.7\_53-26.1  
vhba-kmp-default-debuginfo-20140629\_k3.16.7\_53-2.26.1  
bbswitch-kmp-desktop-0.8\_k3.16.7\_53-3.26.1  
crash-kmp-pae-debuginfo-7.0.8\_k3.16.7\_53-26.1  
virtualbox-qt-debuginfo-5.0.30-62.1  
virtualbox-qt-5.0.30-62.1  
pcfclock-kmp-default-0.44\_k3.16.7\_53-260.26.1  
vhba-kmp-pae-debuginfo-20140629\_k3.16.7\_53-2.26.1  
cloop-kmp-pae-2.639\_k3.16.7\_53-14.26.1  
crash-devel-7.0.8-26.1  
virtualbox-host-kmp-desktop-5.0.30\_k3.16.7\_53-62.1  
cloop-kmp-default-debuginfo-2.639\_k3.16.7\_53-14.26.1  
kernel-obs-build-debugsource-3.16.7-53.2  
bbswitch-kmp-xen-debuginfo-0.8\_k3.16.7\_53-3.26.1  
cloop-kmp-desktop-2.639\_k3.16.7\_53-14.26.1  
crash-debuginfo-7.0.8-26.1  
bbswitch-kmp-desktop-debuginfo-0.8\_k3.16.7\_53-3.26.1  
virtualbox-debugsource-5.0.30-62.1  
kernel-ec2-devel-3.16.7-53.1  
virtualbox-devel-5.0.30-62.1  
hdjmod-kmp-xen-debuginfo-1.28\_k3.16.7\_53-18.27.1  
crash-kmp-pae-7.0.8\_k3.16.7\_53-26.1  
xen-debugsource-4.4.4\_05-55.1  
virtualbox-guest-kmp-default-5.0.30\_k3.16.7\_53-62.1  
xtables-addons-kmp-xen-debuginfo-2.6\_k3.16.7\_53-28.1  
crash-eppic-7.0.8-26.1  
hdjmod-kmp-xen-1.28\_k3.16.7\_53-18.27.1  
python-virtualbox-debuginfo-5.0.30-62.1  
cloop-debuginfo-2.639-14.26.1  
hdjmod-kmp-pae-1.28\_k3.16.7\_53-18.27.1  
virtualbox-debuginfo-5.0.30-62.1  
cloop-debugsource-2.639-14.26.1  
virtualbox-guest-kmp-desktop-debuginfo-5.0.30\_k3.16.7\_53-62.1  
hdjmod-kmp-desktop-debuginfo-1.28\_k3.16.7\_53-18.27.1  
xtables-addons-debugsource-2.6-28.1  
pcfclock-kmp-pae-0.44\_k3.16.7\_53-260.26.1  
kernel-default-base-debuginfo-3.16.7-53.1  
ipset-kmp-xen-debuginfo-6.23\_k3.16.7\_53-26.1  
pcfclock-0.44-260.26.1  
xen-tools-domU-4.4.4\_05-55.1  
hdjmod-kmp-default-debuginfo-1.28\_k3.16.7\_53-18.27.1  
libipset3-6.23-26.1  
virtualbox-host-kmp-default-5.0.30\_k3.16.7\_53-62.1  
virtualbox-guest-x11-debuginfo-5.0.30-62.1  
vhba-kmp-xen-20140629\_k3.16.7\_53-2.26.1  
xtables-addons-kmp-desktop-debuginfo-2.6\_k3.16.7\_53-28.1  
ipset-debugsource-6.23-26.1

i686

kernel-desktop-base-3.16.7-53.1  
kernel-pae-debugsource-3.16.7-53.1  
kernel-vanilla-debugsource-3.16.7-53.1  
kernel-pae-base-debuginfo-3.16.7-53.1  
kernel-ec2-debuginfo-3.16.7-53.1  
kernel-xen-debugsource-3.16.7-53.1  
kernel-desktop-debugsource-3.16.7-53.1  
kernel-ec2-base-debuginfo-3.16.7-53.1  
kernel-desktop-base-debuginfo-3.16.7-53.1  
kernel-pae-debuginfo-3.16.7-53.1  
kernel-desktop-devel-3.16.7-53.1  
kernel-xen-3.16.7-53.1  
kernel-debug-base-debuginfo-3.16.7-53.1  
kernel-pae-devel-3.16.7-53.1  
kernel-debug-3.16.7-53.1  
kernel-xen-base-debuginfo-3.16.7-53.1  
kernel-xen-debuginfo-3.16.7-53.1  
kernel-desktop-debuginfo-3.16.7-53.1  
kernel-ec2-debugsource-3.16.7-53.1  
kernel-vanilla-3.16.7-53.1  
kernel-pae-3.16.7-53.1  
kernel-debug-devel-debuginfo-3.16.7-53.1  
kernel-debug-base-3.16.7-53.1  
kernel-debug-devel-3.16.7-53.1  
kernel-vanilla-debuginfo-3.16.7-53.1  
kernel-vanilla-devel-3.16.7-53.1  
kernel-xen-devel-3.16.7-53.1  
kernel-debug-debugsource-3.16.7-53.1  
kernel-xen-base-3.16.7-53.1  
kernel-desktop-3.16.7-53.1  
kernel-pae-base-3.16.7-53.1  
kernel-debug-debuginfo-3.16.7-53.1

noarch

kernel-docs-3.16.7-53.2  
kernel-source-3.16.7-53.1  
kernel-devel-3.16.7-53.1  
kernel-macros-3.16.7-53.1  
virtualbox-host-source-5.0.30-62.1  
virtualbox-guest-desktop-icons-5.0.30-62.1  
kernel-source-vanilla-3.16.7-53.1

x86\_64

pcfclock-debuginfo-0.44-260.26.1  
hdjmod-kmp-xen-debuginfo-1.28\_k3.16.7\_53-18.27.1  
kernel-default-base-3.16.7-53.1  
xtables-addons-debugsource-2.6-28.1

## 145065 - SuSE Linux 13.1 openSUSE-SU-2016:3077-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8632, CVE-2016-8655, CVE-2016-9555

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3077-1

## Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00064.html>

SuSE Linux 13.1

i586

virtualbox-4.2.36-2.70.1

ndiswrapper-kmp-desktop-debuginfo-1.58\_k3.12.67\_61-39.1

xtables-addons-kmp-xen-2.3\_k3.12.67\_61-2.37.1

pcfclock-kmp-default-0.44\_k3.12.67\_61-258.39.1

hdjmod-kmp-default-debuginfo-1.28\_k3.12.67\_61-16.38.1

crash-7.0.2-2.38.1

vhba-kmp-pae-20130607\_k3.12.67\_61-2.38.1

kernel-syms-3.12.67-61.1

iscsitarget-kmp-default-debuginfo-1.4.20.3\_k3.12.67\_61-13.38.1

pcfclock-kmp-pae-debuginfo-0.44\_k3.12.67\_61-258.39.1

ipset-kmp-default-6.21.1\_k3.12.67\_61-2.42.1

virtualbox-guest-x11-debuginfo-4.2.36-2.70.1

iscsitarget-kmp-xen-debuginfo-1.4.20.3\_k3.12.67\_61-13.38.1

virtualbox-devel-4.2.36-2.70.1

virtualbox-websrv-debuginfo-4.2.36-2.70.1

openvswitch-switch-1.11.0-0.45.1

virtualbox-debugsource-4.2.36-2.70.1

ndiswrapper-debugsource-1.58-39.1

python-openvswitch-1.11.0-0.45.1

openvswitch-kmp-xen-debuginfo-1.11.0\_k3.12.67\_61-0.45.1

iscsitarget-kmp-desktop-1.4.20.3\_k3.12.67\_61-13.38.1

kernel-default-debuginfo-3.12.67-61.1

iscsitarget-debuginfo-1.4.20.3-13.38.1

hdjmod-kmp-pae-1.28\_k3.12.67\_61-16.38.1

kernel-default-devel-3.12.67-61.1

hdjmod-debugsource-1.28-16.38.1

hdjmod-kmp-default-1.28\_k3.12.67\_61-16.38.1

xtables-addons-kmp-desktop-2.3\_k3.12.67\_61-2.37.1

virtualbox-debuginfo-4.2.36-2.70.1

hdjmod-kmp-xen-1.28\_k3.12.67\_61-16.38.1

xen-kmp-pae-4.3.4\_10\_k3.12.67\_61-71.1

hdjmod-kmp-desktop-1.28\_k3.12.67\_61-16.38.1

iscsitarget-debugsource-1.4.20.3-13.38.1

xen-libs-debuginfo-4.3.4\_10-71.1

crash-kmp-default-debuginfo-7.0.2\_k3.12.67\_61-2.38.1

virtualbox-host-kmp-pae-4.2.36\_k3.12.67\_61-2.70.1

openvswitch-test-1.11.0-0.45.1

ipset-kmp-desktop-debuginfo-6.21.1\_k3.12.67\_61-2.42.1

crash-doc-7.0.2-2.38.1

cloop-2.639-11.38.1

pcfclock-kmp-desktop-debuginfo-0.44\_k3.12.67\_61-258.39.1

xen-libs-4.3.4\_10-71.1

openvswitch-kmp-xen-1.11.0\_k3.12.67\_61-0.45.1

xtables-addons-kmp-xen-debuginfo-2.3\_k3.12.67\_61-2.37.1

virtualbox-guest-kmp-desktop-4.2.36\_k3.12.67\_61-2.70.1

cloop-kmp-default-debuginfo-2.639\_k3.12.67\_61-11.38.1

vhba-kmp-default-20130607\_k3.12.67\_61-2.38.1

pcfclock-0.44-258.39.1

ndiswrapper-kmp-desktop-1.58\_k3.12.67\_61-39.1

vhba-kmp-desktop-debuginfo-20130607\_k3.12.67\_61-2.38.1

xen-debugsource-4.3.4\_10-71.1

virtualbox-guest-kmp-default-debuginfo-4.2.36\_k3.12.67\_61-2.70.1



kernel-default-base-debuginfo-3.12.67-61.1  
crash-kmp-desktop-7.0.2\_k3.12.67\_61-2.38.1  
xen-kmp-default-4.3.4\_10\_k3.12.67\_61-71.1  
iscsitarget-kmp-xen-1.4.20.3\_k3.12.67\_61-13.38.1  
ipset-kmp-pae-6.21.1\_k3.12.67\_61-2.42.1  
crash-debuginfo-7.0.2-2.38.1  
openvswitch-pki-1.11.0-0.45.1  
crash-devel-7.0.2-2.38.1  
xtables-addons-kmp-pae-debuginfo-2.3\_k3.12.67\_61-2.37.1  
cloop-debugsource-2.639-11.38.1  
xtables-addons-debuginfo-2.3-2.37.1  
xen-kmp-desktop-debuginfo-4.3.4\_10\_k3.12.67\_61-71.1  
ndiswrapper-kmp-default-debuginfo-1.58\_k3.12.67\_61-39.1  
vhba-kmp-pae-debuginfo-20130607\_k3.12.67\_61-2.38.1  
virtualbox-host-kmp-desktop-debuginfo-4.2.36\_k3.12.67\_61-2.70.1  
cloop-kmp-xen-debuginfo-2.639\_k3.12.67\_61-11.38.1  
cloop-kmp-desktop-debuginfo-2.639\_k3.12.67\_61-11.38.1  
ndiswrapper-kmp-pae-debuginfo-1.58\_k3.12.67\_61-39.1  
virtualbox-host-kmp-default-4.2.36\_k3.12.67\_61-2.70.1  
virtualbox-guest-kmp-pae-4.2.36\_k3.12.67\_61-2.70.1  
openvswitch-1.11.0-0.45.1  
vhba-kmp-xen-20130607\_k3.12.67\_61-2.38.1  
xen-devel-4.3.4\_10-71.1  
virtualbox-websrv-4.2.36-2.70.1  
xen-tools-domU-debuginfo-4.3.4\_10-71.1  
openvswitch-kmp-desktop-debuginfo-1.11.0\_k3.12.67\_61-0.45.1  
kernel-default-3.12.67-61.1  
iscsitarget-1.4.20.3-13.38.1  
cloop-debuginfo-2.639-11.38.1  
openvswitch-debuginfo-1.11.0-0.45.1  
openvswitch-kmp-desktop-1.11.0\_k3.12.67\_61-0.45.1  
ipset-devel-6.21.1-2.42.1  
ipset-kmp-desktop-6.21.1\_k3.12.67\_61-2.42.1  
virtualbox-guest-tools-debuginfo-4.2.36-2.70.1  
pcfclock-kmp-desktop-0.44\_k3.12.67\_61-258.39.1  
cloop-kmp-desktop-2.639\_k3.12.67\_61-11.38.1  
iscsitarget-kmp-pae-1.4.20.3\_k3.12.67\_61-13.38.1  
ipset-6.21.1-2.42.1  
libipset3-6.21.1-2.42.1  
python-virtualbox-debuginfo-4.2.36-2.70.1  
ndiswrapper-debuginfo-1.58-39.1  
python-virtualbox-4.2.36-2.70.1  
ipset-debuginfo-6.21.1-2.42.1  
cloop-kmp-xen-2.639\_k3.12.67\_61-11.38.1  
virtualbox-host-kmp-pae-debuginfo-4.2.36\_k3.12.67\_61-2.70.1  
xtables-addons-debugsource-2.3-2.37.1  
virtualbox-host-kmp-default-debuginfo-4.2.36\_k3.12.67\_61-2.70.1  
kernel-default-base-3.12.67-61.1  
crash-debugsource-7.0.2-2.38.1  
hdjmod-kmp-xen-debuginfo-1.28\_k3.12.67\_61-16.38.1  
xtables-addons-kmp-pae-2.3\_k3.12.67\_61-2.37.1  
ipset-kmp-xen-6.21.1\_k3.12.67\_61-2.42.1  
crash-kmp-xen-7.0.2\_k3.12.67\_61-2.38.1  
openvswitch-switch-debuginfo-1.11.0-0.45.1  
cloop-kmp-pae-debuginfo-2.639\_k3.12.67\_61-11.38.1  
virtualbox-host-kmp-desktop-4.2.36\_k3.12.67\_61-2.70.1  
virtualbox-guest-kmp-pae-debuginfo-4.2.36\_k3.12.67\_61-2.70.1  
virtualbox-guest-tools-4.2.36-2.70.1  
pcfclock-kmp-pae-0.44\_k3.12.67\_61-258.39.1  
pcfclock-kmp-default-debuginfo-0.44\_k3.12.67\_61-258.39.1

iscsitarget-kmp-desktop-debuginfo-1.4.20.3\_k3.12.67\_61-13.38.1  
iscsitarget-kmp-pae-debuginfo-1.4.20.3\_k3.12.67\_61-13.38.1  
pcfclock-debugsource-0.44-258.39.1  
xen-kmp-desktop-4.3.4\_10\_k3.12.67\_61-71.1  
crash-kmp-pae-7.0.2\_k3.12.67\_61-2.38.1  
ipset-debugsource-6.21.1-2.42.1  
cloop-kmp-pae-2.639\_k3.12.67\_61-11.38.1  
vhba-kmp-debugsource-20130607-2.38.1  
xtables-addons-kmp-desktop-debuginfo-2.3\_k3.12.67\_61-2.37.1  
openvswitch-controller-debuginfo-1.11.0-0.45.1  
crash-kmp-pae-debuginfo-7.0.2\_k3.12.67\_61-2.38.1  
crash-gcore-7.0.2-2.38.1  
xen-kmp-pae-debuginfo-4.3.4\_10\_k3.12.67\_61-71.1  
virtualbox-guest-kmp-default-4.2.36\_k3.12.67\_61-2.70.1  
hdjmod-kmp-desktop-debuginfo-1.28\_k3.12.67\_61-16.38.1  
vhba-kmp-desktop-20130607\_k3.12.67\_61-2.38.1  
xtables-addons-kmp-default-debuginfo-2.3\_k3.12.67\_61-2.37.1  
iscsitarget-kmp-default-1.4.20.3\_k3.12.67\_61-13.38.1  
xtables-addons-2.3-2.37.1  
libipset3-debuginfo-6.21.1-2.42.1  
ipset-kmp-default-debuginfo-6.21.1\_k3.12.67\_61-2.42.1  
vhba-kmp-xen-debuginfo-20130607\_k3.12.67\_61-2.38.1  
kernel-default-debugsource-3.12.67-61.1  
ipset-kmp-xen-debuginfo-6.21.1\_k3.12.67\_61-2.42.1  
openvswitch-kmp-default-1.11.0\_k3.12.67\_61-0.45.1  
cloop-kmp-default-2.639\_k3.12.67\_61-11.38.1  
crash-eppic-debuginfo-7.0.2-2.38.1  
virtualbox-qt-4.2.36-2.70.1  
openvswitch-kmp-pae-debuginfo-1.11.0\_k3.12.67\_61-0.45.1  
virtualbox-qt-debuginfo-4.2.36-2.70.1  
xen-kmp-default-debuginfo-4.3.4\_10\_k3.12.67\_61-71.1  
crash-kmp-desktop-debuginfo-7.0.2\_k3.12.67\_61-2.38.1  
python-openvswitch-test-1.11.0-0.45.1  
pcfclock-debuginfo-0.44-258.39.1  
ndiswrapper-kmp-default-1.58\_k3.12.67\_61-39.1  
xtables-addons-kmp-default-2.3\_k3.12.67\_61-2.37.1  
xen-tools-domU-4.3.4\_10-71.1  
crash-eppic-7.0.2-2.38.1  
openvswitch-kmp-pae-1.11.0\_k3.12.67\_61-0.45.1  
openvswitch-controller-1.11.0-0.45.1  
crash-gcore-debuginfo-7.0.2-2.38.1  
virtualbox-guest-kmp-desktop-debuginfo-4.2.36\_k3.12.67\_61-2.70.1  
ndiswrapper-1.58-39.1  
openvswitch-debugsource-1.11.0-0.45.1  
virtualbox-guest-x11-4.2.36-2.70.1  
hdjmod-kmp-pae-debuginfo-1.28\_k3.12.67\_61-16.38.1  
crash-kmp-xen-debuginfo-7.0.2\_k3.12.67\_61-2.38.1  
ipset-kmp-pae-debuginfo-6.21.1\_k3.12.67\_61-2.42.1

## 145077 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:3039-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8632, CVE-2016-8655, CVE-2016-9555

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3039-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002444.html>

### SuSE SLES 12 SP1

noarch

kernel-source-3.12.67-60.64.21.1

kernel-devel-3.12.67-60.64.21.1

kernel-macros-3.12.67-60.64.21.1

x86\_64

kernel-xen-3.12.67-60.64.21.1

kernel-default-3.12.67-60.64.21.1

kernel-xen-debugsource-3.12.67-60.64.21.1

kernel-default-debugsource-3.12.67-60.64.21.1

kernel-syms-3.12.67-60.64.21.1

kernel-default-base-debuginfo-3.12.67-60.64.21.1

kernel-default-base-3.12.67-60.64.21.1

kernel-xen-debuginfo-3.12.67-60.64.21.1

kernel-xen-devel-3.12.67-60.64.21.1

kernel-xen-base-debuginfo-3.12.67-60.64.21.1

kernel-default-debuginfo-3.12.67-60.64.21.1

kernel-xen-base-3.12.67-60.64.21.1

kernel-default-devel-3.12.67-60.64.21.1

### SuSE SLED 12 SP1

x86\_64

kernel-xen-debuginfo-3.12.67-60.64.21.1

kernel-syms-3.12.67-60.64.21.1

kernel-default-extra-3.12.67-60.64.21.1

kernel-default-extra-debuginfo-3.12.67-60.64.21.1

kernel-xen-3.12.67-60.64.21.1

kernel-default-debuginfo-3.12.67-60.64.21.1

kernel-xen-debugsource-3.12.67-60.64.21.1

kernel-default-debugsource-3.12.67-60.64.21.1

kernel-default-devel-3.12.67-60.64.21.1

kernel-xen-devel-3.12.67-60.64.21.1

kernel-default-3.12.67-60.64.21.1

noarch

kernel-source-3.12.67-60.64.21.1

kernel-devel-3.12.67-60.64.21.1

kernel-macros-3.12.67-60.64.21.1

## **145081 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3049-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8632, CVE-2016-8655, CVE-2016-9555

## Description

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

SUSE-SU-2016:3049-1

## Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002452.html>

SuSE SLED 12 SP2

x86\_64

kernel-default-devel-4.4.21-84.1

kernel-default-extra-4.4.21-84.1

kernel-default-4.4.21-84.1

kernel-default-debuginfo-4.4.21-84.1

kernel-default-extra-debuginfo-4.4.21-84.1

kernel-default-debugsource-4.4.21-84.1

kernel-syms-4.4.21-84.1

noarch

kernel-source-4.4.21-84.1

kernel-macros-4.4.21-84.1

kernel-devel-4.4.21-84.1

SuSE SLES 12 SP2

noarch

kernel-source-4.4.21-84.1

kernel-macros-4.4.21-84.1

kernel-devel-4.4.21-84.1

x86\_64

kernel-default-base-4.4.21-84.1

kernel-default-4.4.21-84.1

kernel-default-devel-4.4.21-84.1

kernel-default-debuginfo-4.4.21-84.1

kernel-default-debugsource-4.4.21-84.1

kernel-syms-4.4.21-84.1

kernel-default-base-debuginfo-4.4.21-84.1

## 163235 - Oracle Enterprise Linux ELSA-2016-3651 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9555

### Description

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

ELSA-2016-3651

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006578.html>

<http://oss.oracle.com/pipermail/el-errata/2016-December/006579.html>

OEL7

x86\_64

kernel-uek-doc-3.8.13-118.15.1.el7uek

kernel-uek-devel-3.8.13-118.15.1.el7uek

kernel-uek-debug-devel-3.8.13-118.15.1.el7uek

kernel-uek-debug-3.8.13-118.15.1.el7uek

dtrace-modules-3.8.13-118.15.1.el7uek-0.4.5-3.el7

kernel-uek-3.8.13-118.15.1.el7uek  
kernel-uek-firmware-3.8.13-118.15.1.el7uek

#### OEL6

x86\_64  
kernel-uek-debug-devel-3.8.13-118.15.1.el6uek  
kernel-uek-3.8.13-118.15.1.el6uek  
dtrace-modules-3.8.13-118.15.1.el6uek-0.4.5-3.el6  
kernel-uek-doc-3.8.13-118.15.1.el6uek  
kernel-uek-debug-3.8.13-118.15.1.el6uek  
kernel-uek-devel-3.8.13-118.15.1.el6uek  
kernel-uek-firmware-3.8.13-118.15.1.el6uek

### 163237 - Oracle Enterprise Linux ELSA-2016-3648 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8650, CVE-2016-9555

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-3648

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006572.html>  
<http://oss.oracle.com/pipermail/el-errata/2016-December/006573.html>

#### OEL7

x86\_64  
kernel-uek-firmware-4.1.12-61.1.22.el7uek  
kernel-uek-doc-4.1.12-61.1.22.el7uek  
kernel-uek-debug-4.1.12-61.1.22.el7uek  
kernel-uek-4.1.12-61.1.22.el7uek  
kernel-uek-debug-devel-4.1.12-61.1.22.el7uek  
kernel-uek-devel-4.1.12-61.1.22.el7uek  
dtrace-modules-4.1.12-61.1.22.el7uek-0.5.3-2.el7

#### OEL6

x86\_64  
kernel-uek-4.1.12-61.1.22.el6uek  
kernel-uek-debug-4.1.12-61.1.22.el6uek  
kernel-uek-debug-devel-4.1.12-61.1.22.el6uek  
kernel-uek-doc-4.1.12-61.1.22.el6uek  
kernel-uek-firmware-4.1.12-61.1.22.el6uek  
kernel-uek-devel-4.1.12-61.1.22.el6uek  
dtrace-modules-4.1.12-61.1.22.el6uek-0.5.3-2.el6

### 163238 - Oracle Enterprise Linux ELSA-2016-3652 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9555

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-3652

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-December/006580.html>  
<http://oss.oracle.com/pipermail/el-errata/2016-December/006581.html>

#### OEL5

x86\_64

kernel-uek-2.6.39-400.293.1.el5uek  
kernel-uek-debug-2.6.39-400.293.1.el5uek  
kernel-uek-firmware-2.6.39-400.293.1.el5uek  
kernel-uek-devel-2.6.39-400.293.1.el5uek  
kernel-uek-debug-devel-2.6.39-400.293.1.el5uek  
kernel-uek-doc-2.6.39-400.293.1.el5uek

i386

kernel-uek-2.6.39-400.293.1.el5uek  
kernel-uek-debug-2.6.39-400.293.1.el5uek  
kernel-uek-firmware-2.6.39-400.293.1.el5uek  
kernel-uek-devel-2.6.39-400.293.1.el5uek  
kernel-uek-debug-devel-2.6.39-400.293.1.el5uek  
kernel-uek-doc-2.6.39-400.293.1.el5uek

#### OEL6

x86\_64

kernel-uek-doc-2.6.39-400.293.1.el6uek  
kernel-uek-debug-devel-2.6.39-400.293.1.el6uek  
kernel-uek-devel-2.6.39-400.293.1.el6uek  
kernel-uek-firmware-2.6.39-400.293.1.el6uek  
kernel-uek-2.6.39-400.293.1.el6uek  
kernel-uek-debug-2.6.39-400.293.1.el6uek

i386

kernel-uek-doc-2.6.39-400.293.1.el6uek  
kernel-uek-debug-devel-2.6.39-400.293.1.el6uek  
kernel-uek-devel-2.6.39-400.293.1.el6uek  
kernel-uek-firmware-2.6.39-400.293.1.el6uek  
kernel-uek-2.6.39-400.293.1.el6uek  
kernel-uek-debug-2.6.39-400.293.1.el6uek

### 178270 - Gentoo Linux GLSA-201612-20 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8863

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-20

#### Observation

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

<https://security.gentoo.org/glsa/201612-20>

Affected packages:  
app-misc/jq < 1.5-r2

### 178272 - Gentoo Linux GLSA-201612-38 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2194, CVE-2016-2195

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-38

#### Observation

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

<https://security.gentoo.org/glsa/201612-38>

Affected packages:  
dev-libs/botan < 1.10.12

### 178295 - Gentoo Linux GLSA-201612-16 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2180, CVE-2016-2183, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306, CVE-2016-7052

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-16

#### Observation

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

<https://security.gentoo.org/glsa/201612-16>

Affected packages:  
dev-libs/openssl < 1.0.2j

### 20945 - Google Chrome Multiple Vulnerabilities Prior To 55.0.2883.75

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

Risk Level: High

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, conduct spoofing attacks or remotely execute arbitrary code.

## **20946 - Google Chrome Multiple Vulnerabilities Prior To 55.0.2883.75**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, conduct spoofing attacks or remotely execute arbitrary code.

## **20947 - Moxa NPort Device Vulnerabilities**

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2016-9348, CVE-2016-9361, CVE-2016-9363, CVE-2016-9365, CVE-2016-9366, CVE-2016-9367, CVE-2016-9369, CVE-2016-9371

### Description

Multiple vulnerabilities are present in some versions of Moxa NPort Device.

### Observation

Moxa NPort Device is a product used for controlling serial devices.

Multiple vulnerabilities are present in some versions of Moxa NPort Device. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code, disclose sensitive information and cause a denial of service condition.

## **145050 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2016:3043-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5597

### Description



The scan detected that the host is missing the following update:  
SUSE-SU-2016:3043-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002447.html>

SuSE SLES 12 SP1

x86\_64

java-1\_7\_1-ibm-jdbc-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-alsa-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-plugin-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-1.7.1\_sr3.60-31.2

SuSE SLES 12 SP2

x86\_64

java-1\_7\_1-ibm-jdbc-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-alsa-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-plugin-1.7.1\_sr3.60-31.2  
java-1\_7\_1-ibm-1.7.1\_sr3.60-31.2

### **145051 - SuSE SLES 11 SP4 SUSE-SU-2016:3041-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5597

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3041-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002446.html>

SuSE SLES 11 SP4

i586

java-1\_7\_1-ibm-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-plugin-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-alsa-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr3.60-19.2

x86\_64

java-1\_7\_1-ibm-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-plugin-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-alsa-1.7.1\_sr3.60-19.2  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr3.60-19.2

### **145053 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2016:3078-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5597

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3078-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002462.html>

SuSE SLES 12 SP1

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr3.21-20.1

java-1\_8\_0-ibm-1.8.0\_sr3.21-20.1

java-1\_8\_0-ibm-alsa-1.8.0\_sr3.21-20.1

SuSE SLES 12 SP2

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr3.21-20.1

java-1\_8\_0-ibm-1.8.0\_sr3.21-20.1

java-1\_8\_0-ibm-alsa-1.8.0\_sr3.21-20.1

### 185518 - Ubuntu Linux 12.04 USN-3154-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

#### Description

The scan detected that the host is missing the following update:  
USN-3154-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003667.html>

Ubuntu 12.04

openjdk-6-jre\_6b40-1.13.12-0ubuntu0.12.04.2

openjdk-6-jre-lib\_6b40-1.13.12-0ubuntu0.12.04.2

icedtea-6-jre-cacao\_6b40-1.13.12-0ubuntu0.12.04.2

openjdk-6-jdk\_6b40-1.13.12-0ubuntu0.12.04.2

icedtea-6-jre-jamvm\_6b40-1.13.12-0ubuntu0.12.04.2

openjdk-6-jre-headless\_6b40-1.13.12-0ubuntu0.12.04.2

### 21025 - (SB10181) McAfee VirusScan Enterprise Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-8016, CVE-2016-8017, CVE-2016-8018, CVE-2016-8019, CVE-2016-8020, CVE-2016-8021, CVE-2016-8022, CVE-2016-8023, CVE-2016-8024, CVE-2016-8025

### Description

Multiple vulnerabilities are present in some versions of McAfee VirusScan Enterprise for Linux.

### Observation

McAfee VirusScan Enterprise for Linux delivers always-on, real-time anti-malware protection for Linux environments.

Multiple vulnerabilities are present in some versions of McAfee VirusScan Enterprise for Linux. The flaws lie in several product components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service condition, conduct spoofing attacks or execute arbitrary code.

## **21018 - (K14614344) F5 BIG-IP Libxml2 Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1840

### Description

A buffer overflow vulnerability is present in libxml2 in some versions of F5 BIG-IP systems.

### Observation

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

A buffer overflow vulnerability is present in libxml2 in some versions of F5 BIG-IP systems. The flaw lies in xmlFAParsePosCharGroup function in libxml2. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition.

## **88829 - Slackware Linux 14.2 SSA:2016-347-01 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8655

### Description

The scan detected that the host is missing the following update:  
SSA:2016-347-01

### Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.931787>

Slackware 14.2

i586

kernel-modules-4.4.38-i586-1

kernel-generic-4.4.38-i586-1

kernel-huge-4.4.38-i586-1

i686

kernel-modules-smp-4.4.38\_smp-i686-1

kernel-huge-smp-4.4.38\_smp-i686-1

kernel-generic-smp-4.4.38\_smp-i686-1

noarch

kernel-source-4.4.38-noarch-1

kernel-source-4.4.38\_smp-noarch-1

kernel-firmware-20161211git-noarch-1

x86\_64

kernel-generic-4.4.38-x86\_64-1

kernel-modules-4.4.38-x86\_64-1

kernel-huge-4.4.38-x86\_64-1

### 132309 - Oracle VM OVMSA-2016-0171 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9637

#### Description

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

OVMSA-2016-0171

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000598.html>

OVM3.3

x86\_64

xen-tools-4.3.0-55.el6.119.62

xen-4.3.0-55.el6.119.62

### 132311 - Oracle VM OVMSA-2016-0172 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9637

#### Description

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

OVMSA-2016-0172

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000599.html>

OVM3.2

x86\_64

xen-tools-4.1.3-25.el5.223.45

xen-4.1.3-25.el5.223.45

xen-devel-4.1.3-25.el5.223.45

### 132312 - Oracle VM OVMSA-2016-0173 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

### Description

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

OVMSA-2016-0173

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000597.html>

OVM3.4

x86\_64

xen-tools-4.4.4-105.0.2.1.el6

xen-4.4.4-105.0.2.1.el6

## 141381 - Red Hat Enterprise Linux RHSA-2016-2919 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

### Description

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

RHSA-2016-2919

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2919.html>

RHEL6D

x86\_64

chromium-browser-debuginfo-55.0.2883.75-1.el6

chromium-browser-55.0.2883.75-1.el6

i386

chromium-browser-debuginfo-55.0.2883.75-1.el6

chromium-browser-55.0.2883.75-1.el6

RHEL6S

x86\_64

chromium-browser-debuginfo-55.0.2883.75-1.el6

chromium-browser-55.0.2883.75-1.el6

i386

chromium-browser-debuginfo-55.0.2883.75-1.el6

chromium-browser-55.0.2883.75-1.el6

RHEL6WS

x86\_64

chromium-browser-debuginfo-55.0.2883.75-1.el6

chromium-browser-55.0.2883.75-1.el6

i386  
chromium-browser-debuginfo-55.0.2883.75-1.el6  
chromium-browser-55.0.2883.75-1.el6

## 145058 - SuSE Linux 13.1 openSUSE-SU-2016:3118-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9576, CVE-2016-9794

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3118-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00082.html>

SuSE Linux 13.1

i586

hdjmod-kmp-desktop-1.28\_k3.12.67\_64-16.40.1  
xtables-addons-kmp-pae-debuginfo-2.3\_k3.12.67\_64-2.39.1  
xtables-addons-kmp-xen-2.3\_k3.12.67\_64-2.39.1  
vhba-kmp-pae-20130607\_k3.12.67\_64-2.40.1  
xtables-addons-kmp-default-debuginfo-2.3\_k3.12.67\_64-2.39.1  
vhba-kmp-xen-20130607\_k3.12.67\_64-2.40.1  
virtualbox-guest-tools-4.2.36-2.72.1  
xen-libs-debuginfo-4.3.4\_10-73.1  
ipset-6.21.1-2.44.1  
vhba-kmp-desktop-20130607\_k3.12.67\_64-2.40.1  
iscsitarget-kmp-desktop-debuginfo-1.4.20.3\_k3.12.67\_64-13.40.1  
cloop-kmp-pae-debuginfo-2.639\_k3.12.67\_64-11.40.1  
ndiswrapper-kmp-pae-1.58\_k3.12.67\_64-41.1  
openvswitch-kmp-default-1.11.0\_k3.12.67\_64-0.47.1  
hdjmod-debugsource-1.28-16.40.1  
ipset-debuginfo-6.21.1-2.44.1  
virtualbox-host-kmp-default-4.2.36\_k3.12.67\_64-2.72.1  
cloop-2.639-11.40.1  
xtables-addons-debuginfo-2.3-2.39.1  
ndiswrapper-kmp-pae-debuginfo-1.58\_k3.12.67\_64-41.1  
pcfclock-debuginfo-0.44-258.41.1  
virtualbox-4.2.36-2.72.1  
xen-kmp-desktop-4.3.4\_10\_k3.12.67\_64-73.1  
xen-debugsource-4.3.4\_10-73.1  
python-openvswitch-test-1.11.0-0.47.1  
ndiswrapper-kmp-default-1.58\_k3.12.67\_64-41.1  
ndiswrapper-kmp-desktop-debuginfo-1.58\_k3.12.67\_64-41.1  
crash-debugsource-7.0.2-2.40.1  
ipset-kmp-xen-6.21.1\_k3.12.67\_64-2.44.1  
openvswitch-switch-debuginfo-1.11.0-0.47.1  
openvswitch-debuginfo-1.11.0-0.47.1  
hdjmod-kmp-default-debuginfo-1.28\_k3.12.67\_64-16.40.1  
iscsitarget-kmp-desktop-1.4.20.3\_k3.12.67\_64-13.40.1  
xen-kmp-pae-4.3.4\_10\_k3.12.67\_64-73.1  
vhba-kmp-pae-debuginfo-20130607\_k3.12.67\_64-2.40.1

openvswitch-kmp-desktop-debuginfo-1.11.0\_k3.12.67\_64-0.47.1  
libipset3-debuginfo-6.21.1-2.44.1  
hdjmod-kmp-default-1.28\_k3.12.67\_64-16.40.1  
crash-kmp-default-debuginfo-7.0.2\_k3.12.67\_64-2.40.1  
vhba-kmp-default-20130607\_k3.12.67\_64-2.40.1  
xen-kmp-pae-debuginfo-4.3.4\_10\_k3.12.67\_64-73.1  
virtualbox-host-kmp-pae-debuginfo-4.2.36\_k3.12.67\_64-2.72.1  
openvswitch-debugsource-1.11.0-0.47.1  
openvswitch-kmp-desktop-1.11.0\_k3.12.67\_64-0.47.1  
kernel-default-3.12.67-64.1  
crash-kmp-xen-7.0.2\_k3.12.67\_64-2.40.1  
openvswitch-kmp-default-debuginfo-1.11.0\_k3.12.67\_64-0.47.1  
crash-eppic-7.0.2-2.40.1  
virtualbox-guest-kmp-desktop-4.2.36\_k3.12.67\_64-2.72.1  
cloop-kmp-desktop-2.639\_k3.12.67\_64-11.40.1  
crash-gcore-debuginfo-7.0.2-2.40.1  
ndiswrapper-debuginfo-1.58-41.1  
openvswitch-controller-debuginfo-1.11.0-0.47.1  
pcfclock-kmp-pae-debuginfo-0.44\_k3.12.67\_64-258.41.1  
ipset-kmp-xen-debuginfo-6.21.1\_k3.12.67\_64-2.44.1  
openvswitch-kmp-pae-debuginfo-1.11.0\_k3.12.67\_64-0.47.1  
ipset-kmp-pae-debuginfo-6.21.1\_k3.12.67\_64-2.44.1  
virtualbox-guest-kmp-default-debuginfo-4.2.36\_k3.12.67\_64-2.72.1  
virtualbox-guest-x11-4.2.36-2.72.1  
iscsitarget-debugsource-1.4.20.3-13.40.1  
crash-kmp-desktop-7.0.2\_k3.12.67\_64-2.40.1  
crash-kmp-default-7.0.2\_k3.12.67\_64-2.40.1  
virtualbox-guest-kmp-pae-4.2.36\_k3.12.67\_64-2.72.1  
openvswitch-kmp-pae-1.11.0\_k3.12.67\_64-0.47.1  
virtualbox-websrv-4.2.36-2.72.1  
iscsitarget-debuginfo-1.4.20.3-13.40.1  
ndiswrapper-kmp-desktop-1.58\_k3.12.67\_64-41.1  
virtualbox-host-kmp-desktop-4.2.36\_k3.12.67\_64-2.72.1  
iscsitarget-kmp-default-debuginfo-1.4.20.3\_k3.12.67\_64-13.40.1  
ndiswrapper-1.58-41.1  
vhba-kmp-debugsource-20130607-2.40.1  
hdjmod-kmp-pae-1.28\_k3.12.67\_64-16.40.1  
kernel-default-debugsource-3.12.67-64.1  
xen-kmp-default-4.3.4\_10\_k3.12.67\_64-73.1  
iscsitarget-kmp-xen-debuginfo-1.4.20.3\_k3.12.67\_64-13.40.1  
crash-debuginfo-7.0.2-2.40.1  
cloop-debuginfo-2.639-11.40.1  
crash-doc-7.0.2-2.40.1  
ipset-debugsource-6.21.1-2.44.1  
virtualbox-host-kmp-default-debuginfo-4.2.36\_k3.12.67\_64-2.72.1  
virtualbox-guest-x11-debuginfo-4.2.36-2.72.1  
xtables-addons-kmp-desktop-debuginfo-2.3\_k3.12.67\_64-2.39.1  
virtualbox-devel-4.2.36-2.72.1  
openvswitch-kmp-xen-debuginfo-1.11.0\_k3.12.67\_64-0.47.1  
iscsitarget-kmp-xen-1.4.20.3\_k3.12.67\_64-13.40.1  
openvswitch-pki-1.11.0-0.47.1  
ipset-kmp-default-debuginfo-6.21.1\_k3.12.67\_64-2.44.1  
openvswitch-kmp-xen-1.11.0\_k3.12.67\_64-0.47.1  
ipset-kmp-desktop-6.21.1\_k3.12.67\_64-2.44.1  
virtualbox-guest-kmp-pae-debuginfo-4.2.36\_k3.12.67\_64-2.72.1  
crash-kmp-desktop-debuginfo-7.0.2\_k3.12.67\_64-2.40.1  
openvswitch-1.11.0-0.47.1  
crash-gcore-7.0.2-2.40.1  
xen-devel-4.3.4\_10-73.1  
crash-kmp-pae-7.0.2\_k3.12.67\_64-2.40.1

xtables-addons-kmp-pae-2.3\_k3.12.67\_64-2.39.1  
crash-7.0.2-2.40.1  
pcfclock-kmp-default-debuginfo-0.44\_k3.12.67\_64-258.41.1  
openvswitch-test-1.11.0-0.47.1  
ndiswrapper-kmp-default-debuginfo-1.58\_k3.12.67\_64-41.1  
hdjmod-kmp-xen-debuginfo-1.28\_k3.12.67\_64-16.40.1  
xtables-addons-kmp-desktop-2.3\_k3.12.67\_64-2.39.1  
crash-kmp-pae-debuginfo-7.0.2\_k3.12.67\_64-2.40.1  
kernel-default-base-3.12.67-64.1  
hdjmod-kmp-pae-debuginfo-1.28\_k3.12.67\_64-16.40.1  
virtualbox-qt-4.2.36-2.72.1  
kernel-default-debuginfo-3.12.67-64.1  
virtualbox-qt-debuginfo-4.2.36-2.72.1  
virtualbox-guest-kmp-default-4.2.36\_k3.12.67\_64-2.72.1  
python-virtualbox-debuginfo-4.2.36-2.72.1  
vhba-kmp-xen-debuginfo-20130607\_k3.12.67\_64-2.40.1  
crash-devel-7.0.2-2.40.1  
openvswitch-switch-1.11.0-0.47.1  
virtualbox-debugsource-4.2.36-2.72.1  
python-virtualbox-4.2.36-2.72.1  
xen-kmp-desktop-debuginfo-4.3.4\_10\_k3.12.67\_64-73.1  
pcfclock-kmp-default-0.44\_k3.12.67\_64-258.41.1  
python-openvswitch-1.11.0-0.47.1  
vhba-kmp-default-debuginfo-20130607\_k3.12.67\_64-2.40.1  
xen-tools-domU-4.3.4\_10-73.1  
hdjmod-kmp-xen-1.28\_k3.12.67\_64-16.40.1  
iscsitarget-kmp-pae-debuginfo-1.4.20.3\_k3.12.67\_64-13.40.1  
pcfclock-kmp-desktop-debuginfo-0.44\_k3.12.67\_64-258.41.1  
kernel-syms-3.12.67-64.1  
pcfclock-kmp-desktop-0.44\_k3.12.67\_64-258.41.1  
virtualbox-debuginfo-4.2.36-2.72.1  
openvswitch-controller-1.11.0-0.47.1  
virtualbox-host-kmp-desktop-debuginfo-4.2.36\_k3.12.67\_64-2.72.1  
cloop-kmp-default-2.639\_k3.12.67\_64-11.40.1  
crash-eppic-debuginfo-7.0.2-2.40.1  
virtualbox-host-kmp-pae-4.2.36\_k3.12.67\_64-2.72.1  
cloop-kmp-xen-2.639\_k3.12.67\_64-11.40.1  
iscsitarget-kmp-pae-1.4.20.3\_k3.12.67\_64-13.40.1  
xtables-addons-kmp-default-2.3\_k3.12.67\_64-2.39.1  
ndiswrapper-debugsource-1.58-41.1  
xen-libs-4.3.4\_10-73.1  
crash-kmp-xen-debuginfo-7.0.2\_k3.12.67\_64-2.40.1  
xtables-addons-2.3-2.39.1  
ipset-kmp-default-6.21.1\_k3.12.67\_64-2.44.1  
ipset-kmp-desktop-debuginfo-6.21.1\_k3.12.67\_64-2.44.1  
iscsitarget-kmp-default-1.4.20.3\_k3.12.67\_64-13.40.1  
hdjmod-kmp-desktop-debuginfo-1.28\_k3.12.67\_64-16.40.1  
pcfclock-0.44-258.41.1  
pcfclock-kmp-pae-0.44\_k3.12.67\_64-258.41.1  
xen-tools-domU-debuginfo-4.3.4\_10-73.1  
xtables-addons-debugsource-2.3-2.39.1  
cloop-kmp-xen-debuginfo-2.639\_k3.12.67\_64-11.40.1  
vhba-kmp-desktop-debuginfo-20130607\_k3.12.67\_64-2.40.1  
cloop-kmp-default-debuginfo-2.639\_k3.12.67\_64-11.40.1  
cloop-debugsource-2.639-11.40.1  
virtualbox-guest-tools-debuginfo-4.2.36-2.72.1  
xtables-addons-kmp-xen-debuginfo-2.3\_k3.12.67\_64-2.39.1  
kernel-default-devel-3.12.67-64.1  
cloop-kmp-desktop-debuginfo-2.639\_k3.12.67\_64-11.40.1  
ipset-kmp-pae-6.21.1\_k3.12.67\_64-2.44.1



ipset-devel-6.21.1-2.44.1  
virtualbox-websrv-debuginfo-4.2.36-2.72.1  
iscsitarget-1.4.20.3-13.40.1  
kernel-default-base-debuginfo-3.12.67-64.1  
cloop-kmp-pae-2.639\_k3.12.67\_64-11.40.1

## 145059 - SuSE Linux 13.2 openSUSE-SU-2016:3059-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7944

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3059-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00056.html>

SuSE Linux 13.2

x86\_64

libXfixes-debugsource-5.0.1-4.3.1

libXfixes3-debuginfo-5.0.1-4.3.1

libXfixes3-debuginfo-32bit-5.0.1-4.3.1

libXfixes-devel-5.0.1-4.3.1

libXfixes3-32bit-5.0.1-4.3.1

libXfixes3-5.0.1-4.3.1

libXfixes-devel-32bit-5.0.1-4.3.1

i586

libXfixes3-5.0.1-4.3.1

libXfixes-devel-5.0.1-4.3.1

libXfixes-debugsource-5.0.1-4.3.1

libXfixes3-debuginfo-5.0.1-4.3.1

## 145060 - SuSE SLES 12 SP1 SUSE-SU-2016:3079-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-6816, CVE-2016-8735

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3079-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002463.html>

SuSE SLES 12 SP1

noarch

tomcat-lib-8.0.32-10.13.2  
tomcat-servlet-3\_1-api-8.0.32-10.13.2  
tomcat-el-3\_0-api-8.0.32-10.13.2  
tomcat-8.0.32-10.13.2  
tomcat-docs-webapp-8.0.32-10.13.2  
tomcat-javadoc-8.0.32-10.13.2  
tomcat-admin-webapps-8.0.32-10.13.2  
tomcat-jsp-2\_3-api-8.0.32-10.13.2  
tomcat-webapps-8.0.32-10.13.2

## 145062 - SuSE SLES 11 SP4 SUSE-SU-2016:3080-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5285, CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-9064, CVE-2016-9066, CVE-2016-9074, CVE-2016-9079

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3080-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002464.html>

SuSE SLES 11 SP4

i586

libfreebl3-3.21.3-39.1

mozilla-nss-tools-3.21.3-39.1

mozilla-nss-3.21.3-39.1

MozillaFirefox-45.5.1esr-59.1

libsoftokn3-3.21.3-39.1

MozillaFirefox-translations-45.5.1esr-59.1

x86\_64

libfreebl3-3.21.3-39.1

mozilla-nss-tools-3.21.3-39.1

libsoftokn3-32bit-3.21.3-39.1

libfreebl3-32bit-3.21.3-39.1

mozilla-nss-3.21.3-39.1

mozilla-nss-32bit-3.21.3-39.1

MozillaFirefox-45.5.1esr-59.1

libsoftokn3-3.21.3-39.1

MozillaFirefox-translations-45.5.1esr-59.1

## 145063 - SuSE SLES 12 SP2 SUSE-SU-2016:3081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797, CVE-2016-6816, CVE-2016-8735

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3081-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002465.html>

SuSE SLES 12 SP2

noarch

tomcat-webapps-8.0.36-17.1

tomcat-servlet-3\_1-api-8.0.36-17.1

tomcat-admin-webapps-8.0.36-17.1

tomcat-javadoc-8.0.36-17.1

tomcat-jsp-2\_3-api-8.0.36-17.1

tomcat-docs-webapp-8.0.36-17.1

tomcat-el-3\_0-api-8.0.36-17.1

tomcat-lib-8.0.36-17.1

tomcat-8.0.36-17.1

## **145064 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3107-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7969, CVE-2016-7970, CVE-2016-7971, CVE-2016-7972

## Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3107-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002475.html>

SuSE SLED 12 SP1

x86\_64

libass5-0.10.2-3.1

libass5-debuginfo-0.10.2-3.1

libass5-debugsource-0.10.2-3.1

SuSE SLES 12 SP2

x86\_64

libass5-0.10.2-3.1

libass5-debuginfo-0.10.2-3.1

libass5-debugsource-0.10.2-3.1

SuSE SLED 12 SP2

x86\_64

libass5-0.10.2-3.1

libass5-debuginfo-0.10.2-3.1

libass5-debugsource-0.10.2-3.1

SuSE SLES 12 SP1

x86\_64

libass5-0.10.2-3.1

libass5-debuginfo-0.10.2-3.1

libass5-debugsource-0.10.2-3.1

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

Risk Level: High

CVE: CVE-2016-9556, CVE-2016-9559

### Description

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

openSUSE-SU-2016:3027-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00043.html>

SuSE Linux 13.2

i586

libMagickWand-6\_Q16-2-debuginfo-6.8.9.8-42.1

libMagickCore-6\_Q16-2-debuginfo-6.8.9.8-42.1

ImageMagick-extra-debuginfo-6.8.9.8-42.1

libMagick++-6\_Q16-5-debuginfo-6.8.9.8-42.1

libMagickCore-6\_Q16-2-6.8.9.8-42.1

ImageMagick-debuginfo-6.8.9.8-42.1

ImageMagick-extra-6.8.9.8-42.1

perl-PerlMagick-debuginfo-6.8.9.8-42.1

libMagick++-6\_Q16-5-6.8.9.8-42.1

ImageMagick-debugsource-6.8.9.8-42.1

perl-PerlMagick-6.8.9.8-42.1

libMagickWand-6\_Q16-2-6.8.9.8-42.1

ImageMagick-6.8.9.8-42.1

libMagick++-devel-6.8.9.8-42.1

ImageMagick-devel-6.8.9.8-42.1

noarch

ImageMagick-doc-6.8.9.8-42.1

x86\_64

libMagickWand-6\_Q16-2-debuginfo-6.8.9.8-42.1

libMagickCore-6\_Q16-2-debuginfo-6.8.9.8-42.1

ImageMagick-extra-debuginfo-6.8.9.8-42.1

ImageMagick-devel-32bit-6.8.9.8-42.1

libMagick++-6\_Q16-5-32bit-6.8.9.8-42.1

libMagick++-6\_Q16-5-debuginfo-6.8.9.8-42.1

libMagickWand-6\_Q16-2-debuginfo-32bit-6.8.9.8-42.1

libMagickCore-6\_Q16-2-6.8.9.8-42.1

ImageMagick-debuginfo-6.8.9.8-42.1

libMagickCore-6\_Q16-2-debuginfo-32bit-6.8.9.8-42.1

ImageMagick-extra-6.8.9.8-42.1

perl-PerlMagick-debuginfo-6.8.9.8-42.1

libMagick++-6\_Q16-5-6.8.9.8-42.1

libMagickCore-6\_Q16-2-32bit-6.8.9.8-42.1

ImageMagick-debugsource-6.8.9.8-42.1

perl-PerlMagick-6.8.9.8-42.1

libMagickWand-6\_Q16-2-32bit-6.8.9.8-42.1

libMagick++-devel-32bit-6.8.9.8-42.1

libMagickWand-6\_Q16-2-6.8.9.8-42.1

ImageMagick-6.8.9.8-42.1

libMagick+-6\_Q16-5-debuginfo-32bit-6.8.9.8-42.1  
libMagick+-devel-6.8.9.8-42.1  
ImageMagick-devel-6.8.9.8-42.1

## 145067 - SuSE Linux 13.2 openSUSE-SU-2016:3026-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9556, CVE-2016-9559

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3026-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00042.html>

SuSE Linux 13.2

x86\_64

libGraphicsMagick3-config-1.3.20-18.1  
libGraphicsMagick-Q16-3-debuginfo-1.3.20-18.1  
perl-GraphicsMagick-1.3.20-18.1  
GraphicsMagick-devel-1.3.20-18.1  
libGraphicsMagick+-Q16-3-debuginfo-1.3.20-18.1  
libGraphicsMagick-Q16-3-1.3.20-18.1  
GraphicsMagick-1.3.20-18.1  
perl-GraphicsMagick-debuginfo-1.3.20-18.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-18.1  
libGraphicsMagick+-devel-1.3.20-18.1  
GraphicsMagick-debugsource-1.3.20-18.1  
libGraphicsMagick+-Q16-3-1.3.20-18.1  
GraphicsMagick-debuginfo-1.3.20-18.1  
libGraphicsMagickWand-Q16-2-1.3.20-18.1

i586

libGraphicsMagick3-config-1.3.20-18.1  
libGraphicsMagick-Q16-3-debuginfo-1.3.20-18.1  
perl-GraphicsMagick-1.3.20-18.1  
GraphicsMagick-devel-1.3.20-18.1  
libGraphicsMagick+-Q16-3-debuginfo-1.3.20-18.1  
libGraphicsMagick-Q16-3-1.3.20-18.1  
GraphicsMagick-1.3.20-18.1  
perl-GraphicsMagick-debuginfo-1.3.20-18.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-18.1  
libGraphicsMagick+-devel-1.3.20-18.1  
GraphicsMagick-debugsource-1.3.20-18.1  
libGraphicsMagick+-Q16-3-1.3.20-18.1  
GraphicsMagick-debuginfo-1.3.20-18.1  
libGraphicsMagickWand-Q16-2-1.3.20-18.1

## 145068 - SuSE SLES 11 SP4 SUSE-SU-2016:3110-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3110-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002477.html>

SuSE SLES 11 SP4  
i586  
xorg-x11-libXv-7.4-1.20.1

x86\_64  
xorg-x11-libXv-7.4-1.20.1  
xorg-x11-libXv-32bit-7.4-1.20.1

**145070 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3057-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-9427

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3057-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002457.html>

SuSE SLED 12 SP1  
x86\_64  
libgc1-7.2d-5.1  
libgc1-debuginfo-7.2d-5.1  
gc-debugsource-7.2d-5.1

SuSE SLES 12 SP2  
x86\_64  
libgc1-7.2d-5.1  
libgc1-debuginfo-7.2d-5.1  
gc-debugsource-7.2d-5.1

SuSE SLED 12 SP2  
x86\_64  
libgc1-7.2d-5.1  
libgc1-debuginfo-7.2d-5.1  
gc-debugsource-7.2d-5.1

SuSE SLES 12 SP1  
x86\_64  
libgc1-7.2d-5.1

libgc1-debuginfo-7.2d-5.1  
gc-debugsource-7.2d-5.1

### 145071 - SuSE SLES 11 SP4 SUSE-SU-2016:3054-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7942

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3054-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002455.html>

SuSE SLES 11 SP4  
i586  
xorg-x11-libX11-7.4-5.11.65.1

x86\_64  
xorg-x11-libX11-32bit-7.4-5.11.65.1  
xorg-x11-libX11-7.4-5.11.65.1

### 145072 - SuSE SLES 11 SP4 SUSE-SU-2016:3115-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7949, CVE-2016-7950

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3115-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002481.html>

SuSE SLES 11 SP4  
i586  
xorg-x11-libXrender-7.4-1.20.1

x86\_64  
xorg-x11-libXrender-32bit-7.4-1.20.1  
xorg-x11-libXrender-7.4-1.20.1

### 145073 - SuSE Linux 13.2 openSUSE-SU-2016:3031-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7953

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3031-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00045.html>

SuSE Linux 13.2

x86\_64

libXvMC-devel-1.0.8-4.3.1

libXvMC1-debuginfo-1.0.8-4.3.1

libXvMC-debugsource-1.0.8-4.3.1

libXvMC1-32bit-1.0.8-4.3.1

libXvMC-devel-32bit-1.0.8-4.3.1

libXvMC1-debuginfo-32bit-1.0.8-4.3.1

libXvMC1-1.0.8-4.3.1

i586

libXvMC-debugsource-1.0.8-4.3.1

libXvMC-devel-1.0.8-4.3.1

libXvMC1-debuginfo-1.0.8-4.3.1

libXvMC1-1.0.8-4.3.1

## 145074 - SuSE Linux 13.2 openSUSE-SU-2016:3108-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3108-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00081.html>

SuSE Linux 13.2

x86\_64

chromedriver-55.0.2883.75-148.1

chromedriver-debuginfo-55.0.2883.75-148.1

chromium-debugsource-55.0.2883.75-148.1

chromium-ffmpegsumo-55.0.2883.75-148.1

chromium-ffmpegsumo-debuginfo-55.0.2883.75-148.1

chromium-debuginfo-55.0.2883.75-148.1

chromium-55.0.2883.75-148.1



i586  
chromedriver-55.0.2883.75-148.1  
chromedriver-debuginfo-55.0.2883.75-148.1  
chromium-debugsource-55.0.2883.75-148.1  
chromium-ffmpegsumo-55.0.2883.75-148.1  
chromium-ffmpegsumo-debuginfo-55.0.2883.75-148.1  
chromium-debuginfo-55.0.2883.75-148.1  
chromium-55.0.2883.75-148.1

### 145075 - SuSE Linux 13.2 openSUSE-SU-2016:3033-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5407

#### Description

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

openSUSE-SU-2016:3033-1

#### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00047.html>

SuSE Linux 13.2

x86\_64

libXv-debugsource-1.0.10-4.3.1

libXv1-debuginfo-1.0.10-4.3.1

libXv-devel-1.0.10-4.3.1

libXv1-32bit-1.0.10-4.3.1

libXv-devel-32bit-1.0.10-4.3.1

libXv1-1.0.10-4.3.1

libXv1-debuginfo-32bit-1.0.10-4.3.1

i586

libXv1-debuginfo-1.0.10-4.3.1

libXv1-1.0.10-4.3.1

libXv-debugsource-1.0.10-4.3.1

libXv-devel-1.0.10-4.3.1

### 145076 - SuSE Linux 13.2 openSUSE-SU-2016:3087-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7969, CVE-2016-7972

#### Description

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

openSUSE-SU-2016:3087-1

#### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00068.html>

SuSE Linux 13.2  
x86\_64  
libass5-debuginfo-0.12.1-2.8.1  
libass5-debuginfo-32bit-0.12.1-2.8.1  
libass5-0.12.1-2.8.1  
libass5-debugsource-0.12.1-2.8.1  
libass5-devel-0.12.1-2.8.1  
libass5-32bit-0.12.1-2.8.1

i586  
libass5-0.12.1-2.8.1  
libass5-devel-0.12.1-2.8.1  
libass5-debuginfo-0.12.1-2.8.1  
libass5-debugsource-0.12.1-2.8.1

### 145078 - SuSE Linux 13.2 openSUSE-SU-2016:3035-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8127, CVE-2015-7554, CVE-2015-8665, CVE-2015-8683, CVE-2016-3622, CVE-2016-3658, CVE-2016-5321, CVE-2016-5323, CVE-2016-5652, CVE-2016-5875, CVE-2016-9273, CVE-2016-9297, CVE-2016-9448, CVE-2016-9453

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3035-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00049.html>

SuSE Linux 13.2  
x86\_64  
libtiff5-debuginfo-4.0.7-10.35.1  
tiff-4.0.7-10.35.1  
tiff-debuginfo-4.0.7-10.35.1  
libtiff-devel-32bit-4.0.7-10.35.1  
libtiff5-debuginfo-32bit-4.0.7-10.35.1  
libtiff-devel-4.0.7-10.35.1  
tiff-debugsource-4.0.7-10.35.1  
libtiff5-4.0.7-10.35.1  
libtiff5-32bit-4.0.7-10.35.1

i586  
libtiff5-debuginfo-4.0.7-10.35.1  
tiff-4.0.7-10.35.1  
tiff-debuginfo-4.0.7-10.35.1  
libtiff-devel-4.0.7-10.35.1  
tiff-debugsource-4.0.7-10.35.1  
libtiff5-4.0.7-10.35.1

### 145079 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3048-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9079

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3048-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002451.html>

SuSE SLED 12 SP1

x86\_64

MozillaFirefox-debuginfo-45.5.1esr-93.1

MozillaFirefox-translations-45.5.1esr-93.1

MozillaFirefox-debugsource-45.5.1esr-93.1

MozillaFirefox-45.5.1esr-93.1

SuSE SLES 12 SP2

x86\_64

MozillaFirefox-debuginfo-45.5.1esr-93.1

MozillaFirefox-translations-45.5.1esr-93.1

MozillaFirefox-debugsource-45.5.1esr-93.1

MozillaFirefox-45.5.1esr-93.1

SuSE SLED 12 SP2

x86\_64

MozillaFirefox-debuginfo-45.5.1esr-93.1

MozillaFirefox-translations-45.5.1esr-93.1

MozillaFirefox-debugsource-45.5.1esr-93.1

MozillaFirefox-45.5.1esr-93.1

SuSE SLES 12 SP1

x86\_64

MozillaFirefox-debuginfo-45.5.1esr-93.1

MozillaFirefox-translations-45.5.1esr-93.1

MozillaFirefox-debugsource-45.5.1esr-93.1

MozillaFirefox-45.5.1esr-93.1

## 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-2016-5103

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3032-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00046.html>

SuSE Linux 13.2

noarch  
roundcubemail-1.0.9-23.1

## 145082 - SuSE Linux 13.2 openSUSE-SU-2016:3037-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7951, CVE-2016-7952

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3037-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00051.html>

SuSE Linux 13.2

x86\_64

libXtst-debugsource-1.2.2-4.3.1

libXtst-devel-1.2.2-4.3.1

libXtst6-debuginfo-1.2.2-4.3.1

libXtst-devel-32bit-1.2.2-4.3.1

libXtst6-1.2.2-4.3.1

libXtst6-32bit-1.2.2-4.3.1

libXtst6-debuginfo-32bit-1.2.2-4.3.1

i586

libXtst6-debuginfo-1.2.2-4.3.1

libXtst6-1.2.2-4.3.1

libXtst-devel-1.2.2-4.3.1

libXtst-debugsource-1.2.2-4.3.1

## 145083 - SuSE Linux 13.2 openSUSE-SU-2016:3034-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7942, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3034-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00048.html>

SuSE Linux 13.2

i586

libxcb-composite0-1.11-2.5.1

libxcb-xevie0-1.11-2.5.1

libxcb-res0-1.11-2.5.1

libxcb-xvnc0-debuginfo-1.11-2.5.1  
libxcb-present0-debuginfo-1.11-2.5.1  
libxcb-xprint0-debuginfo-1.11-2.5.1  
libxcb-xf86dri0-1.11-2.5.1  
libxcb-record0-1.11-2.5.1  
libxcb-glx0-1.11-2.5.1  
libxcb-render0-debuginfo-1.11-2.5.1  
libxcb-dri2-0-1.11-2.5.1  
libxcb1-debuginfo-1.11-2.5.1  
libxcb-xf86dri0-debuginfo-1.11-2.5.1  
libxcb-shm0-debuginfo-1.11-2.5.1  
libxcb-shape0-1.11-2.5.1  
libxcb-debugsource-1.11-2.5.1  
libxcb-xtest0-debuginfo-1.11-2.5.1  
libX11-devel-1.6.2-5.6.1  
libXi-debugsource-1.7.4-2.3.1  
libxcb-screensaver0-debuginfo-1.11-2.5.1  
libxcb-xinerama0-debuginfo-1.11-2.5.1  
libxcb-damage0-1.11-2.5.1  
libxcb-xtest0-1.11-2.5.1  
libxcb-sync1-1.11-2.5.1  
libxcb-xfixes0-debuginfo-1.11-2.5.1  
libxcb-record0-debuginfo-1.11-2.5.1  
libxcb-composite0-debuginfo-1.11-2.5.1  
libX11-xcb1-1.6.2-5.6.1  
libxcb-xevie0-debuginfo-1.11-2.5.1  
libxcb-screensaver0-1.11-2.5.1  
libxcb-sync1-debuginfo-1.11-2.5.1  
libXi6-debuginfo-1.7.4-2.3.1  
libxcb-devel-1.11-2.5.1  
libXrandr2-debuginfo-1.4.2-4.3.1  
libxcb-dri2-0-debuginfo-1.11-2.5.1  
libxcb-xprint0-1.11-2.5.1  
libXi6-1.7.4-2.3.1  
libxcb-xfixes0-1.11-2.5.1  
libXrandr-debugsource-1.4.2-4.3.1  
libxcb-xkb1-1.11-2.5.1  
libxcb-randr0-1.11-2.5.1  
libXrandr-devel-1.4.2-4.3.1  
libxcb-shm0-1.11-2.5.1  
libXrandr2-1.4.2-4.3.1  
libX11-6-1.6.2-5.6.1  
libxcb-render0-1.11-2.5.1  
libxcb-dri3-0-1.11-2.5.1  
libX11-xcb1-debuginfo-1.6.2-5.6.1  
libxcb-glx0-debuginfo-1.11-2.5.1  
libxcb-xv0-debuginfo-1.11-2.5.1  
libxcb-dri3-0-debuginfo-1.11-2.5.1  
libxcb-shape0-debuginfo-1.11-2.5.1  
libxcb1-1.11-2.5.1  
libxcb-xv0-1.11-2.5.1  
libxcb-dpms0-1.11-2.5.1  
libX11-6-debuginfo-1.6.2-5.6.1  
libxcb-xkb1-debuginfo-1.11-2.5.1  
libX11-debugsource-1.6.2-5.6.1  
libxcb-res0-debuginfo-1.11-2.5.1  
libXi-devel-1.7.4-2.3.1  
libxcb-dpms0-debuginfo-1.11-2.5.1  
libxcb-randr0-debuginfo-1.11-2.5.1  
libxcb-damage0-debuginfo-1.11-2.5.1

libxcb-xvnc0-1.11-2.5.1  
libxcb-xinerama0-1.11-2.5.1  
libxcb-present0-1.11-2.5.1

noarch

libxcb-devel-doc-1.11-2.5.1  
libX11-data-1.6.2-5.6.1

x86\_64

libxcb-glx0-32bit-1.11-2.5.1  
libXi6-32bit-1.7.4-2.3.1  
libxcb-damage0-debuginfo-32bit-1.11-2.5.1  
libxcb-composite0-1.11-2.5.1  
libxcb-shape0-32bit-1.11-2.5.1  
libxcb-xevie0-1.11-2.5.1  
libxcb-screensaver0-32bit-1.11-2.5.1  
libxcb-composite0-32bit-1.11-2.5.1  
libxcb-dri2-0-debuginfo-32bit-1.11-2.5.1  
libxcb-res0-1.11-2.5.1  
libxcb-xvnc0-debuginfo-1.11-2.5.1  
libxcb-present0-debuginfo-1.11-2.5.1  
libxcb-xprint0-debuginfo-1.11-2.5.1  
libxcb-xf86dri0-1.11-2.5.1  
libxcb-record0-1.11-2.5.1  
libxcb-glx0-1.11-2.5.1  
libxcb-damage0-32bit-1.11-2.5.1  
libxcb-render0-debuginfo-1.11-2.5.1  
libxcb-dri2-0-1.11-2.5.1  
libxcb-xinerama0-debuginfo-32bit-1.11-2.5.1  
libxcb1-debuginfo-1.11-2.5.1  
libxcb-record0-32bit-1.11-2.5.1  
libxcb-xprint0-32bit-1.11-2.5.1  
libxcb-xinerama0-32bit-1.11-2.5.1  
libxcb-xvnc0-32bit-1.11-2.5.1  
libxcb-xf86dri0-debuginfo-1.11-2.5.1  
libxcb-composite0-debuginfo-32bit-1.11-2.5.1  
libxcb-shm0-debuginfo-1.11-2.5.1  
libxcb-shape0-1.11-2.5.1  
libxcb-xfixes0-32bit-1.11-2.5.1  
libxcb-shm0-32bit-1.11-2.5.1  
libxcb-randr0-32bit-1.11-2.5.1  
libxcb-debugsource-1.11-2.5.1  
libxcb-glx0-debuginfo-32bit-1.11-2.5.1  
libxcb-devel-32bit-1.11-2.5.1  
libxcb-xtest0-32bit-1.11-2.5.1  
libXrandr-devel-32bit-1.4.2-4.3.1  
libxcb-present0-32bit-1.11-2.5.1  
libxcb-xtest0-debuginfo-1.11-2.5.1  
libX11-devel-1.6.2-5.6.1  
libxcb-xevie0-32bit-1.11-2.5.1  
libxcb-record0-debuginfo-32bit-1.11-2.5.1  
libxcb-render0-32bit-1.11-2.5.1  
libxcb-xv0-32bit-1.11-2.5.1  
libXi-debugsource-1.7.4-2.3.1  
libxcb-screensaver0-debuginfo-1.11-2.5.1  
libXrandr2-debuginfo-32bit-1.4.2-4.3.1  
libX11-xcb1-debuginfo-32bit-1.6.2-5.6.1  
libxcb-res0-32bit-1.11-2.5.1  
libxcb-xfixes0-debuginfo-32bit-1.11-2.5.1  
libxcb-xinerama0-debuginfo-1.11-2.5.1

libxcb-damage0-1.11-2.5.1  
libxcb-xtest0-1.11-2.5.1  
libxcb-xf86dri0-32bit-1.11-2.5.1  
libxcb-sync1-1.11-2.5.1  
libxcb-xfixes0-debuginfo-1.11-2.5.1  
libxcb-record0-debuginfo-1.11-2.5.1  
libxcb-xprint0-debuginfo-32bit-1.11-2.5.1  
libxcb-composite0-debuginfo-1.11-2.5.1  
libX11-xcb1-1.6.2-5.6.1  
libxcb-xvmc0-debuginfo-32bit-1.11-2.5.1  
libXi6-debuginfo-32bit-1.7.4-2.3.1  
libxcb-xevie0-debuginfo-1.11-2.5.1  
libxcb-screensaver0-1.11-2.5.1  
libxcb-sync1-debuginfo-1.11-2.5.1  
libxcb-xevie0-debuginfo-32bit-1.11-2.5.1  
libxcb-dri3-0-debuginfo-32bit-1.11-2.5.1  
libXi6-debuginfo-1.7.4-2.3.1  
libxcb-devel-1.11-2.5.1  
libXrandr2-debuginfo-1.4.2-4.3.1  
libxcb-xv0-debuginfo-32bit-1.11-2.5.1  
libX11-devel-32bit-1.6.2-5.6.1  
libxcb-dri2-0-debuginfo-1.11-2.5.1  
libxcb-xkb1-debuginfo-32bit-1.11-2.5.1  
libxcb-xprint0-1.11-2.5.1  
libxcb-shape0-debuginfo-32bit-1.11-2.5.1  
libXi6-1.7.4-2.3.1  
libxcb-xfixes0-1.11-2.5.1  
libXrandr-debugsource-1.4.2-4.3.1  
libX11-6-32bit-1.6.2-5.6.1  
libxcb-xkb1-1.11-2.5.1  
libX11-xcb1-32bit-1.6.2-5.6.1  
libxcb-sync1-32bit-1.11-2.5.1  
libxcb-dri3-0-32bit-1.11-2.5.1  
libxcb-randr0-1.11-2.5.1  
libXrandr-devel-1.4.2-4.3.1  
libxcb-dri2-0-32bit-1.11-2.5.1  
libxcb-dpms0-debuginfo-32bit-1.11-2.5.1  
libxcb-shm0-1.11-2.5.1  
libXrandr2-1.4.2-4.3.1  
libX11-6-1.6.2-5.6.1  
libxcb-render0-1.11-2.5.1  
libxcb-xtest0-debuginfo-32bit-1.11-2.5.1  
libxcb-screensaver0-debuginfo-32bit-1.11-2.5.1  
libxcb-dri3-0-1.11-2.5.1  
libX11-xcb1-debuginfo-1.6.2-5.6.1  
libxcb1-32bit-1.11-2.5.1  
libxcb-glx0-debuginfo-1.11-2.5.1  
libxcb-xv0-debuginfo-1.11-2.5.1  
libxcb-dri3-0-debuginfo-1.11-2.5.1  
libxcb-present0-debuginfo-32bit-1.11-2.5.1  
libxcb-randr0-debuginfo-32bit-1.11-2.5.1  
libxcb-shape0-debuginfo-1.11-2.5.1  
libXrandr2-32bit-1.4.2-4.3.1  
libxcb-sync1-debuginfo-32bit-1.11-2.5.1  
libxcb1-1.11-2.5.1  
libxcb-xv0-1.11-2.5.1  
libxcb1-debuginfo-32bit-1.11-2.5.1  
libxcb-dpms0-1.11-2.5.1  
libxcb-dpms0-32bit-1.11-2.5.1  
libX11-6-debuginfo-1.6.2-5.6.1

libxcb-xkb1-debuginfo-1.11-2.5.1  
libX11-debugsource-1.6.2-5.6.1  
libxcb-res0-debuginfo-1.11-2.5.1  
libXi-devel-1.7.4-2.3.1  
libX11-6-debuginfo-32bit-1.6.2-5.6.1  
libxcb-xf86dri0-debuginfo-32bit-1.11-2.5.1  
libxcb-xkb1-32bit-1.11-2.5.1  
libxcb-dpms0-debuginfo-1.11-2.5.1  
libxcb-res0-debuginfo-32bit-1.11-2.5.1  
libxcb-randr0-debuginfo-1.11-2.5.1  
libxcb-damage0-debuginfo-1.11-2.5.1  
libxcb-shm0-debuginfo-32bit-1.11-2.5.1  
libxcb-xvmc0-1.11-2.5.1  
libxcb-xinerama0-1.11-2.5.1  
libxcb-render0-debuginfo-32bit-1.11-2.5.1  
libXi-devel-32bit-1.7.4-2.3.1  
libxcb-present0-1.11-2.5.1

### 145084 - SuSE SLES 11 SP4 SUSE-SU-2016:3069-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-7513, CVE-2016-0823, CVE-2016-3841, CVE-2016-4997, CVE-2016-4998, CVE-2016-5195, CVE-2016-5696, CVE-2016-6480, CVE-2016-6828, CVE-2016-7425

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3069-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002461.html>

SuSE SLES 11 SP4

x86\_64

kernel-syms-rt-3.0.101.rt130-65.1

kernel-rt-base-3.0.101.rt130-65.1

kernel-source-rt-3.0.101.rt130-65.1

kernel-rt\_trace-devel-3.0.101.rt130-65.1

kernel-rt-3.0.101.rt130-65.1

kernel-rt\_trace-3.0.101.rt130-65.1

kernel-rt\_trace-base-3.0.101.rt130-65.1

kernel-rt-devel-3.0.101.rt130-65.1

### 145085 - SuSE Linux 13.2 openSUSE-SU-2016:3036-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7949, CVE-2016-7950

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:3036-1



### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00050.html>

SuSE Linux 13.2

x86\_64

libXrender-debugsource-0.9.8-4.3.1

libXrender-devel-32bit-0.9.8-4.3.1

libXrender1-debuginfo-32bit-0.9.8-4.3.1

libXrender1-debuginfo-0.9.8-4.3.1

libXrender1-0.9.8-4.3.1

libXrender1-32bit-0.9.8-4.3.1

libXrender-devel-0.9.8-4.3.1

i586

libXrender1-debuginfo-0.9.8-4.3.1

libXrender-devel-0.9.8-4.3.1

libXrender1-0.9.8-4.3.1

libXrender-debugsource-0.9.8-4.3.1

### **160178 - CentOS 5, 6 CESA-2016-2850 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-9079

### Description

The scan detected that the host is missing the following update:  
CESA-2016-2850

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-December/022170.html>

<http://lists.centos.org/pipermail/centos-announce/2016-December/022169.html>

CentOS 5

x86\_64

thunderbird-45.5.1-1.el5.centos

i386

thunderbird-45.5.1-1.el5.centos

CentOS 6

x86\_64

thunderbird-45.5.1-1.el6.centos

i686

thunderbird-45.5.1-1.el6.centos

### **170749 - Amazon Linux AMI ALAS-2016-772 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8645, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084

### Description

The scan detected that the host is missing the following update:  
ALAS-2016-772

### Observation

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

<https://alas.aws.amazon.com/ALAS-2016-772.html>

Amazon Linux AMI

i686  
perf-4.4.35-33.55.amzn1  
kernel-tools-4.4.35-33.55.amzn1  
kernel-debuginfo-4.4.35-33.55.amzn1  
kernel-4.4.35-33.55.amzn1  
kernel-tools-debuginfo-4.4.35-33.55.amzn1  
kernel-headers-4.4.35-33.55.amzn1  
kernel-devel-4.4.35-33.55.amzn1  
kernel-tools-devel-4.4.35-33.55.amzn1  
perf-debuginfo-4.4.35-33.55.amzn1  
kernel-debuginfo-common-i686-4.4.35-33.55.amzn1

noarch

kernel-doc-4.4.35-33.55.amzn1

x86\_64

kernel-debuginfo-common-x86\_64-4.4.35-33.55.amzn1  
perf-4.4.35-33.55.amzn1  
kernel-tools-4.4.35-33.55.amzn1  
kernel-debuginfo-4.4.35-33.55.amzn1  
kernel-4.4.35-33.55.amzn1  
kernel-tools-debuginfo-4.4.35-33.55.amzn1  
kernel-headers-4.4.35-33.55.amzn1  
kernel-devel-4.4.35-33.55.amzn1  
kernel-tools-devel-4.4.35-33.55.amzn1  
perf-debuginfo-4.4.35-33.55.amzn1

## **178269 - Gentoo Linux GLSA-201612-30 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8145

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-30

### Observation

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

<https://security.gentoo.org/glsa/201612-30>

Affected packages:

media-sound/sox < 14.4.2

### 178275 - Gentoo Linux GLSA-201612-29 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-2892

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-29

#### Observation

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

<https://security.gentoo.org/glsa/201612-29>

Affected packages:

media-libs/libmms < 0.6.4

### 178276 - Gentoo Linux GLSA-201612-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9390, CVE-2014-9462, CVE-2016-3068, CVE-2016-3069, CVE-2016-3105, CVE-2016-3630

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-19

#### Observation

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

<https://security.gentoo.org/glsa/201612-19>

Affected packages:

dev-vcs/mercurial < 3.8.4

### 178279 - Gentoo Linux GLSA-201612-25 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6318

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-25

#### Observation

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

<https://security.gentoo.org/glsa/201612-25>

Affected packages:

sys-libs/cracklib < 2.9.6-r1

### 178280 - Gentoo Linux GLSA-201612-36 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-6051, CVE-2014-8240

#### Description

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

GLSA-201612-36

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-36>

Affected packages:

net-misc/tigervnc < 1.4.2

### 178281 - Gentoo Linux GLSA-201612-26 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-1923, CVE-2016-1924, CVE-2016-3181, CVE-2016-3182, CVE-2016-3183, CVE-2016-7445

#### Description

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

GLSA-201612-26

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-26>

Affected packages:

media-libs/openjpeg < 2.1.1\_p20160922

### 178283 - Gentoo Linux GLSA-201612-27 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0981, CVE-2014-0983, CVE-2014-6588, CVE-2014-6589, CVE-2014-6590, CVE-2014-6595, CVE-2015-0377, CVE-2015-0418, CVE-2015-0427, CVE-2015-3456, CVE-2016-5608, CVE-2016-5610, CVE-2016-5611, CVE-2016-5613

#### Description

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

GLSA-201612-27

### Observation

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

<https://security.gentoo.org/glsa/201612-27>

Affected packages:

app-emulation/virtualbox < 4.3.28

app-emulation/virtualbox-bin < 4.3.28

### **178286 - Gentoo Linux GLSA-201612-21 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-7036

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-21

### Observation

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

<https://security.gentoo.org/glsa/201612-21>

Affected packages:

dev-db/sqlite < 3.11.1

### **178289 - Gentoo Linux GLSA-201612-22 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-9471

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-22

### Observation

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

<https://security.gentoo.org/glsa/201612-22>

Affected packages:

sys-apps/coreutils < 8.23

### **178291 - Gentoo Linux GLSA-201612-18 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8325, CVE-2016-1908, CVE-2016-3115, CVE-2016-6210, CVE-2016-8858

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-18

### Observation

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

<https://security.gentoo.org/glsa/201612-18>

Affected packages:

net-misc/openssh < 7.3\_p1-r7

## **178292 - Gentoo Linux GLSA-201612-34 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-4391, CVE-2013-4393, CVE-2013-4394

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-34

### Observation

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

<https://security.gentoo.org/glsa/201612-34>

Affected packages:

sys-apps/systemd < 208

## **178293 - Gentoo Linux GLSA-201612-24 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-24

### Observation

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

<https://security.gentoo.org/glsa/201612-24>

Affected packages:

sys-devel/binutils < 2.25

## **191460 - Fedora Linux 25 FEDORA-2016-722c0afc64 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6911, CVE-2016-7568, CVE-2016-8670

#### Description

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

FEDORA-2016-722c0afc64

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

gd-2.2.3-5.fc25

### **191477 - Fedora Linux 24 FEDORA-2016-b601141219 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6318

#### Description

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

FEDORA-2016-b601141219

#### 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/2016/12/?count=200&page=2>

Fedora Core 24

cracklib-2.9.6-4.fc24

### **191479 - Fedora Linux 24 FEDORA-2016-5cb5b4082d Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8655, CVE-2016-9576, CVE-2016-9793

#### Description

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

FEDORA-2016-5cb5b4082d

#### 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/2016/12/?count=200&page=1>

Fedora Core 24

kernel-4.8.13-200.fc24

### 191492 - Fedora Linux 23 FEDORA-2016-8d79ade826 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6354

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-8d79ade826

#### 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/2016/12/?count=200&page=3>

Fedora Core 23

flex-2.6.0-2.fc23

### 191493 - Fedora Linux 25 FEDORA-2016-107f03cc00 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8655, CVE-2016-9576, CVE-2016-9793

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-107f03cc00

#### 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/2016/12/?count=200&page=1>

Fedora Core 25

kernel-4.8.13-300.fc25

### 191494 - Fedora Linux 25 FEDORA-2016-bfa785e39e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6318

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-bfa785e39e



### 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/2016/12/?count=200&page=2>

Fedora Core 25

cracklib-2.9.6-4.fc25

### **191497 - Fedora Linux 23 FEDORA-2016-5aff4a6bbc Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8655, CVE-2016-9576, CVE-2016-9793

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-5aff4a6bbc

### 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/2016/12/?count=200&page=1>

Fedora Core 23

kernel-4.8.13-100.fc23

### **21013 - Apache ActiveMQ Web Console Cross-Site Scripting Vulnerability**

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

Risk Level: Medium

CVE: CVE-2016-6810

### Description

A vulnerability is present in some versions of Apache ActiveMQ.

### Observation

Apache ActiveMQ is an open source messaging server.

A vulnerability is present in some versions of Apache ActiveMQ. The flaw is due to improper user data output validation. Successful exploitation could allow an attacker to remotely execute arbitrary script.

### **21014 - Ipswitch WhatsUp Gold SQL Injection Vulnerability**

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

Risk Level: Medium

CVE: CVE-2016-1000000

### Description

A SQL Injection vulnerability is present in some versions of Ipswitch WhatsUp Gold.

### Observation

Ipswitch WhatsUp Gold is a network management and monitoring software for Windows environments.

A SQL Injection vulnerability is present in some versions of Ipswitch WhatsUp Gold. The flaw is due to improper validation of user inputs in some fields. Successful exploitation by an attacker could lead to the disclosure of sensitive information.

## **21015 - (CTX219136) Citrix XenServer QEMU ioport Array Overflow Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-9637

### Description

A privilege escalation vulnerability is present in some versions of Citrix XenServer.

### Observation

Citrix XenServer is a popular virtualization platform.

A privilege escalation vulnerability is present in some versions of Citrix XenServer. The flaw lie in QEMU. Successful exploitation could allow an attacker to escalate their privilege and compromise the host.

## **21016 - IBM WebSphere Application Server Admin Console Cross-Site Scripting Vulnerability**

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

Risk Level: Medium

CVE: CVE-2016-8934

### Description

A cross-site scripting vulnerability is present in some versions of IBM WebSphere Application Server,

### Observation

IBM WebSphere Application Server is a Java application server.

A cross-site scripting vulnerability is present in some versions of IBM WebSphere Application Server, The flaw lies in Admin Console. Successful exploitation could allow an attacker to execute arbitrary JavaScript code.

## **145052 - SuSE SLES 11 SP4 SUSE-SU-2016:3046-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2010-2074, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9621, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3046-1

### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002449.html>

SuSE SLES 11 SP4

i586

w3m-0.5.3.git20161120-4.1

x86\_64

w3m-0.5.3.git20161120-4.1

### 145057 - SuSE Linux 13.2 openSUSE-SU-2016:3090-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1251

#### Description

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

openSUSE-SU-2016:3090-1

#### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-12/msg00071.html>

SuSE Linux 13.2

x86\_64

perl-DBD-mysql-debuginfo-4.021-8.3.1

perl-DBD-mysql-debugsource-4.021-8.3.1

perl-DBD-mysql-4.021-8.3.1

i586

perl-DBD-mysql-debuginfo-4.021-8.3.1

perl-DBD-mysql-debugsource-4.021-8.3.1

perl-DBD-mysql-4.021-8.3.1

### 178268 - Gentoo Linux GLSA-201612-40 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-4024, CVE-2012-4025

#### Description

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

GLSA-201612-40

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-40>

Affected packages:

squashfs-tools < 4.3

## 178285 - Gentoo Linux GLSA-201612-41 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4412, CVE-2014-4413, CVE-2014-4414

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-41

### Observation

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

<https://security.gentoo.org/glsa/201612-41>

Affected packages:

net-libs/webkit-gtk < 2.4.10-r200

## 178288 - Gentoo Linux GLSA-201612-32 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-0172

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-32

### Observation

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

<https://security.gentoo.org/glsa/201612-32>

Affected packages:

dev-libs/elfutils < 0.159

## 178290 - Gentoo Linux GLSA-201612-33 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3228

### Description

The scan detected that the host is missing the following update:  
GLSA-201612-33

### Observation

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

<https://security.gentoo.org/glsa/201612-33>

Affected packages:  
app-text/ghostscript-gpl < 9.09

#### 191453 - Fedora Linux 24 FEDORA-2016-60753c3dcd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9920

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-60753c3dcd

##### 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/2016/12/?count=200&page=1>

Fedora Core 24

roundcubemail-1.2.3-1.fc24

#### 191455 - Fedora Linux 25 FEDORA-2016-673cbb6bb4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1249, CVE-2016-1251

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-673cbb6bb4

##### 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/2016/12/?count=200&page=1>

Fedora Core 25

perl-DBD-MySQL-4.041-1.fc25

#### 191482 - Fedora Linux 24 FEDORA-2016-302f840ecf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1251

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-302f840ecf

### 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/2016/12/?count=200&page=3>

Fedora Core 24

perl-DBD-MySQL-4.039-2.fc24

### **191487 - Fedora Linux 25 FEDORA-2016-d361d188d9 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-9920

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-d361d188d9

### 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/2016/12/?count=200&page=3>

Fedora Core 25

roundcubemail-1.2.3-1.fc25

### **20950 - IBM WebSphere Application Server SOAP Information Disclosure Vulnerability (swg21991469)**

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

### Description

An information disclosure vulnerability is present in some versions of IBM WebSphere Application Server.

### Observation

IBM WebSphere Application Server is a Java application server.

An information disclosure vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in processing of SOAP requests. Successful exploitation could allow an attacker to obtain sensitive information.

### **20954 - (K52638558) F5 BIG-IP RESOLV::lookup Irule Command Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-6876

### Description

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

### 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 products. The flaw lies in the RESOLV::lookup IRule command. Successful exploitation could allow an attacker to cause a denial of service condition.

### **20955 - (SOL82679059) F5 BIG-IP BIG-IP APM SSO Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-3686

### Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP systems.

### Observation

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

An information disclosure vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the sso feature. Successful exploitation could allow an attacker to obtain sensitive information.

### **21017 - (SB10180) McAfee Endpoint Security Web Control Cross-Site Scripting Vulnerability**

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

Risk Level: Medium

CVE: CVE-2016-8011

### Description

A cross-site scripting vulnerability is present in some versions of McAfee Endpoint Security Web Control.

### Observation

McAfee Endpoint Security Web Control is McAfee websites access control.

A cross-site scripting vulnerability is present in some versions of McAfee Endpoint Security Web Control. The flaw lies within the block or warn pages. Successful exploitation could allow an attacker to execute arbitrary JavaScript code.

### **21026 - Moxa MiiNePort Session Hijack Vulnerabilities**

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: Medium

CVE: CVE-2016-9344, CVE-2016-9346

### Description

Multiple vulnerabilities are present in some versions of Moxa MiinePort Device.

### Observation

Moxa MiiNePort Device is a product used for controlling serial devices.

Multiple vulnerabilities are present in some versions of Moxa MiiNePort Device. The flaws lie in several components. Successful exploitation could allow an attacker to use brute-force on an active session cookie and gain access to configuration files which are not encrypted, there by gain unrestricted privileges and access to the device.

## 132313 - Oracle VM OVMSA-2016-0170 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

### Description

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

OVMSA-2016-0170

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000596.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-December/000595.html>

OVM3.3

x86\_64

sudo-1.8.6p3-25.el6\_8

OVM3.4

x86\_64

sudo-1.8.6p3-25.el6\_8

## 145054 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3047-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7945, CVE-2016-7946

### Description

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

SUSE-SU-2016:3047-1

### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002450.html>

SuSE SLED 12 SP1

x86\_64

libXi-debugsource-1.7.4-17.1

libXi6-32bit-1.7.4-17.1

libXi6-debuginfo-32bit-1.7.4-17.1

libXi6-1.7.4-17.1

libXi6-debuginfo-1.7.4-17.1

SuSE SLES 12 SP2

x86\_64

libXi-debugsource-1.7.4-17.1

libXi6-debuginfo-1.7.4-17.1

libXi6-debuginfo-32bit-1.7.4-17.1

libXi6-1.7.4-17.1



libXi6-32bit-1.7.4-17.1

SuSE SLED 12 SP2

x86\_64

libXi6-debugsource-1.7.4-17.1

libXi6-32bit-1.7.4-17.1

libXi6-debuginfo-32bit-1.7.4-17.1

libXi6-1.7.4-17.1

libXi6-debuginfo-1.7.4-17.1

SuSE SLES 12 SP1

x86\_64

libXi6-debugsource-1.7.4-17.1

libXi6-debuginfo-1.7.4-17.1

libXi6-debuginfo-32bit-1.7.4-17.1

libXi6-1.7.4-17.1

libXi6-32bit-1.7.4-17.1

### 160177 - CentOS 6 CESA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

#### Description

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

CESA-2016-2872

#### Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-December/022171.html>

CentOS 6

x86\_64

sudo-devel-1.8.6p3-25.el6\_8

sudo-1.8.6p3-25.el6\_8

i686

sudo-devel-1.8.6p3-25.el6\_8

sudo-1.8.6p3-25.el6\_8

### 163236 - Oracle Enterprise Linux ELSA-2016-2872 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7032, CVE-2016-7076

#### Description

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

ELSA-2016-2872

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-December/006553.html>  
<http://oss.oracle.com/pipermail/el-errata/2016-December/006554.html>

OEL7  
x86\_64  
sudo-devel-1.8.6p7-21.el7\_3  
sudo-1.8.6p7-21.el7\_3

OEL6  
x86\_64  
sudo-devel-1.8.6p3-25.el6\_8  
sudo-1.8.6p3-25.el6\_8

i386  
sudo-devel-1.8.6p3-25.el6\_8  
sudo-1.8.6p3-25.el6\_8

### 178271 - Gentoo Linux GLSA-201612-43 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8027, CVE-2016-2086, CVE-2016-2216, CVE-2016-5325

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-43

#### Observation

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

<https://security.gentoo.org/glsa/201612-43>

Affected packages:  
net-libs/nodejs < 4.6.1

### 178274 - Gentoo Linux GLSA-201612-39 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0634

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-39

#### Observation

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

<https://security.gentoo.org/glsa/201612-39>

Affected packages:  
app-shells/bash < 4.3\_p46-r1

---

## 178277 - Gentoo Linux GLSA-201612-23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

### Description

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

GLSA-201612-23

### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-23>

Affected packages:

net-misc/socat < 1.7.3.1

## 178278 - Gentoo Linux GLSA-201612-31 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8026

### Description

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

GLSA-201612-31

### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-31>

Affected packages:

sys-fs/exfat-utils < 1.2.1

## 178282 - Gentoo Linux GLSA-201612-37 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

### Description

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

GLSA-201612-37

### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-37>

Affected packages:  
x11-libs/pixman < 0.32.8

### 178284 - Gentoo Linux GLSA-201612-17 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes  
Risk Level: Medium  
CVE: CVE-2016-5873

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-17

#### Observation

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

<https://security.gentoo.org/glsa/201612-17>

Affected packages:  
dev-php/pecl-http < 2.5.6

### 178287 - Gentoo Linux GLSA-201612-42 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes  
Risk Level: Medium  
CVE: CVE-2016-4338, CVE-2016-9140

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-42

#### Observation

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

<https://security.gentoo.org/glsa/201612-42>

Affected packages:  
net-analyzer/zabbix < 2.2.16

### 178294 - Gentoo Linux GLSA-201612-35 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes  
Risk Level: Medium  
CVE: CVE-2013-7285

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-35

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201612-35>

Affected packages:

dev-java/xstream < 1.4.8-r1

### 182210 - FreeBSD cryptopp Multiple Vulnerabilities (eab68cff-bc0c-11e6-b2ca-001b3856973b)

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

Risk Level: Medium

CVE: CVE-2015-2141, CVE-2016-3995, CVE-2016-7420

#### Description

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

cryptopp -- multiple vulnerabilities (eab68cff-bc0c-11e6-b2ca-001b3856973b)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/eab68cff-bc0c-11e6-b2ca-001b3856973b.html>

Affected packages:

cryptopp < 5.6.5

### 191454 - Fedora Linux 25 FEDORA-2016-260d22944d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8740

#### Description

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

FEDORA-2016-260d22944d

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

httpd-2.4.23-5.fc25

### 191471 - Fedora Linux 24 FEDORA-2016-b39fedec11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8740

#### Description

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

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/2016/12/?count=200&page=2>

Fedora Core 24

httpd-2.4.23-5.fc24

**145055 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:3067-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7777, CVE-2016-7908, CVE-2016-7909, CVE-2016-8667, CVE-2016-8669, CVE-2016-8910, CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9384, CVE-2016-9385, CVE-2016-9386, CVE-2016-9637

Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3067-1

Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002459.html>

SuSE SLED 12 SP2

x86\_64

xen-libs-debuginfo-4.7.1\_02-25.1

xen-libs-debuginfo-32bit-4.7.1\_02-25.1

xen-libs-4.7.1\_02-25.1

xen-libs-32bit-4.7.1\_02-25.1

xen-debugsource-4.7.1\_02-25.1

xen-4.7.1\_02-25.1

SuSE SLES 12 SP2

x86\_64

xen-libs-debuginfo-4.7.1\_02-25.1

xen-doc-html-4.7.1\_02-25.1

xen-libs-debuginfo-32bit-4.7.1\_02-25.1

xen-tools-domU-4.7.1\_02-25.1

xen-tools-4.7.1\_02-25.1

xen-tools-domU-debuginfo-4.7.1\_02-25.1

xen-libs-4.7.1\_02-25.1

xen-libs-32bit-4.7.1\_02-25.1

xen-debugsource-4.7.1\_02-25.1

xen-tools-debuginfo-4.7.1\_02-25.1

xen-4.7.1\_02-25.1

**145061 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:3083-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7777, CVE-2016-7908, CVE-2016-7909, CVE-2016-7995, CVE-2016-8576, CVE-2016-8667, CVE-2016-8669, CVE-2016-8909, CVE-2016-8910, CVE-2016-9377, CVE-2016-9378, CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386, CVE-2016-9637

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3083-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002466.html>

#### SuSE SLES 12 SP1

x86\_64  
xen-libs-debuginfo-4.5.5\_02-22.3.1  
xen-kmp-default-debuginfo-4.5.5\_02\_k3.12.67\_60.64.18-22.3.1  
xen-4.5.5\_02-22.3.1  
xen-tools-domU-debuginfo-4.5.5\_02-22.3.1  
xen-kmp-default-4.5.5\_02\_k3.12.67\_60.64.18-22.3.1  
xen-debugsource-4.5.5\_02-22.3.1  
xen-doc-html-4.5.5\_02-22.3.1  
xen-libs-32bit-4.5.5\_02-22.3.1  
xen-libs-debuginfo-32bit-4.5.5\_02-22.3.1  
xen-libs-4.5.5\_02-22.3.1  
xen-tools-debuginfo-4.5.5\_02-22.3.1  
xen-tools-domU-4.5.5\_02-22.3.1  
xen-tools-4.5.5\_02-22.3.1

#### SuSE SLED 12 SP1

x86\_64  
xen-libs-debuginfo-32bit-4.5.5\_02-22.3.1  
xen-kmp-default-debuginfo-4.5.5\_02\_k3.12.67\_60.64.18-22.3.1  
xen-debugsource-4.5.5\_02-22.3.1  
xen-kmp-default-4.5.5\_02\_k3.12.67\_60.64.18-22.3.1  
xen-libs-4.5.5\_02-22.3.1  
xen-libs-32bit-4.5.5\_02-22.3.1  
xen-4.5.5\_02-22.3.1  
xen-libs-debuginfo-4.5.5\_02-22.3.1

### 145069 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:3053-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9621, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:3053-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-December/002454.html>

SuSE SLED 12 SP1

x86\_64

w3m-debugsource-0.5.3.git20161120-160.1

w3m-debuginfo-0.5.3.git20161120-160.1

w3m-0.5.3.git20161120-160.1

SuSE SLES 12 SP2

x86\_64

w3m-debugsource-0.5.3.git20161120-160.1

w3m-debuginfo-0.5.3.git20161120-160.1

w3m-0.5.3.git20161120-160.1

SuSE SLED 12 SP2

x86\_64

w3m-debugsource-0.5.3.git20161120-160.1

w3m-debuginfo-0.5.3.git20161120-160.1

w3m-0.5.3.git20161120-160.1

SuSE SLES 12 SP1

x86\_64

w3m-debugsource-0.5.3.git20161120-160.1

w3m-debuginfo-0.5.3.git20161120-160.1

w3m-0.5.3.git20161120-160.1

### 191483 - Fedora Linux 25 FEDORA-2016-6ba1694d89 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9888

#### Description

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

FEDORA-2016-6ba1694d89

#### 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/2016/12/?count=200&page=2>

Fedora Core 25

libgsf-1.14.33-4.fc25

### 88827 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-347-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9933, CVE-2016-9934, CVE-2016-9935

#### Description

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

SSA:2016-347-03



### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.429698>

Slackware 14.0  
x86\_64  
php-5.6.29-x86\_64-1

Slackware 14.2  
x86\_64  
php-5.6.29-x86\_64-1

i586  
php-5.6.29-i586-1

Slackware 14.1  
x86\_64  
php-5.6.29-x86\_64-1

### **88828 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-347-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9928

### Description

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

SSA:2016-347-02

### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.458719>

Slackware 14.0  
x86\_64  
mcabber-1.0.4-x86\_64-1

Slackware 14.2  
x86\_64  
mcabber-1.0.4-x86\_64-1

i586  
mcabber-1.0.4-i586-1

Slackware 14.1  
x86\_64  
mcabber-1.0.4-x86\_64-1

### **130643 - Debian Linux 8.0 DSA-3730-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-9066, CVE-2016-9074, CVE-2016-9079

#### Description

The scan detected that the host is missing the following update:  
DSA-3730-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3730>

Debian 8.0  
all  
icedove\_1:45.5.1-1~deb8u1

### **130644 - Debian Linux 8.0 DSA-3731-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198, CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202, CVE-2016-5203, CVE-2016-5204, CVE-2016-5205, CVE-2016-5206, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5210, CVE-2016-5211, CVE-2016-5212, CVE-2016-5213, CVE-2016-5214, CVE-2016-5215, CVE-2016-5216, CVE-2016-5217, CVE-2016-5218, CVE-2016-5219, CVE-2016-5220, CVE-2016-5221, CVE-2016-5222, CVE-2016-5223, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

#### Description

The scan detected that the host is missing the following update:  
DSA-3731-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3731>

Debian 8.0  
all  
chromedriver\_55.0.2883.75-1~deb8u1  
chromium-inspector\_55.0.2883.75-1~deb8u1  
chromium-dbg\_55.0.2883.75-1~deb8u1  
chromium-l10n\_55.0.2883.75-1~deb8u1  
chromium\_55.0.2883.75-1~deb8u1

### **130645 - Debian Linux 8.0 DSA-3732-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9138, CVE-2016-9933, CVE-2016-9934

#### Description

The scan detected that the host is missing the following update:  
DSA-3732-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3732>

Debian 8.0  
all  
php5\_5.6.28+dfsg-0+deb8u1

### **130646 - Debian Linux 8.0 DSA-3733-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-1252

### Description

The scan detected that the host is missing the following update:  
DSA-3733-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3733>

Debian 8.0  
all  
apt\_1.0.9.8.4

### **130647 - Debian Linux 8.0 DSA-3729-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7777, CVE-2016-9379, CVE-2016-9380, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386

### Description

The scan detected that the host is missing the following update:  
DSA-3729-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3729>

Debian 8.0  
all  
xen-utils-common\_4.4.1-9+deb8u8  
libxen-dev\_4.4.1-9+deb8u8  
xen-utils-4.4\_4.4.1-9+deb8u8  
xen-system-armhf\_4.4.1-9+deb8u8  
xen-hypervisor-4.4-arm64\_4.4.1-9+deb8u8  
xen-hypervisor-4.4-armhf\_4.4.1-9+deb8u8  
libxen-4.4\_4.4.1-9+deb8u8

xen-system-arm64\_4.4.1-9+deb8u8  
libxenstore3.0\_4.4.1-9+deb8u8  
xen-system-amd64\_4.4.1-9+deb8u8  
xen-hypervisor-4.4-amd64\_4.4.1-9+deb8u8  
xenstore-utils\_4.4.1-9+deb8u8

### 182208 - FreeBSD PHP Multiple Vulnerabilities (2d56308b-c0a8-11e6-a9a5-b499baebfeaf)

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:  
PHP -- Multiple vulnerabilities (2d56308b-c0a8-11e6-a9a5-b499baebfeaf)

#### Observation

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

<http://www.vuxml.org/freebsd/2d56308b-c0a8-11e6-a9a5-b499baebfeaf.html>

Affected packages:

php56 < 5.6.29

php70 < 7.0.14

### 182209 - FreeBSD asterisk Authentication Bypass (c0b13887-be44-11e6-b04f-001999f8d30b)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
asterisk -- Authentication Bypass (c0b13887-be44-11e6-b04f-001999f8d30b)

#### Observation

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

<http://www.vuxml.org/freebsd/c0b13887-be44-11e6-b04f-001999f8d30b.html>

Affected packages:

asterisk11 < 11.25.1

asterisk13 < 13.13.1

### 182211 - FreeBSD FreeBSD Link\_ntoa (3) buffer overflow (0282269d-bbee-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-6559

#### Description

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

FreeBSD -- link\_ntoa(3) buffer overflow (0282269d-bbee-11e6-b1cf-14dae9d210b8)

### Observation

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

<http://www.vuxml.org/freebsd/0282269d-bbee-11e6-b1cf-14dae9d210b8.html>

Affected packages:

11.0 <= FreeBSD < 11.0\_5  
10.3 <= FreeBSD < 10.3\_14  
10.2 <= FreeBSD < 10.2\_27  
10.1 <= FreeBSD < 10.1\_44  
9.3 <= FreeBSD < 9.3\_52

## **182212 - FreeBSD asterisk Crash On SDP Offer Or Answer From Endpoint Using Opus (9e6640fe-be3a-11e6-b04f-001999f8d30b)**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
asterisk -- Crash on SDP offer or answer from endpoint using Opus (9e6640fe-be3a-11e6-b04f-001999f8d30b)

### Observation

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

<http://www.vuxml.org/freebsd/9e6640fe-be3a-11e6-b04f-001999f8d30b.html>

Affected packages:

13.12.0 <= asterisk13 < 13.13.1

## **182213 - FreeBSD FreeBSD Possible Login (1) argument injection in telnetd(8) (e00304d2-bbed-11e6-b1cf-14dae9d210b8)**

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

Risk Level: Low

CVE: CVE-2016-1888

### Description

The scan detected that the host is missing the following update:  
FreeBSD -- Possible login(1) argument injection in telnetd(8) (e00304d2-bbed-11e6-b1cf-14dae9d210b8)

### Observation

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

<http://www.vuxml.org/freebsd/e00304d2-bbed-11e6-b1cf-14dae9d210b8.html>

Affected packages:

11.0 <= FreeBSD < 11.0\_4  
10.3 <= FreeBSD < 10.3\_13  
10.2 <= FreeBSD < 10.2\_26

10.1 <= FreeBSD < 10.1\_43

9.3 <= FreeBSD < 9.3\_51

### 182214 - FreeBSD FreeBSD Bhyve (8) virtual machine escape (e722e3c6-bbee-11e6-b1cf-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2016-1889

#### Description

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

FreeBSD -- bhyve(8) virtual machine escape (e722e3c6-bbee-11e6-b1cf-14dae9d210b8)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/e722e3c6-bbee-11e6-b1cf-14dae9d210b8.html>

Affected packages:

11.0 <= FreeBSD < 11.0\_4

10.3 <= FreeBSD < 10.3\_13

10.2 <= FreeBSD < 10.2\_26

10.1 <= FreeBSD < 10.1\_43

### 185519 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3153-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5204, CVE-2016-5205, CVE-2016-5207, CVE-2016-5208, CVE-2016-5209, CVE-2016-5212, CVE-2016-5213, CVE-2016-5215, CVE-2016-5219, CVE-2016-5221, CVE-2016-5222, CVE-2016-5224, CVE-2016-5225, CVE-2016-5226, CVE-2016-9650, CVE-2016-9651, CVE-2016-9652

#### Description

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

USN-3153-1

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003668.html>

Ubuntu 16.04

liboxideqtcore0\_1.19.4-0ubuntu0.16.04.1

Ubuntu 14.04

liboxideqtcore0\_1.19.4-0ubuntu0.14.04.1

Ubuntu 16.10

liboxideqtcore0\_1.19.4-0ubuntu0.16.10.1

## 185520 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3155-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904

### Description

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

USN-3155-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003670.html>

Ubuntu 12.04

firefox\_50.1.0+build2-0ubuntu0.12.04.1

Ubuntu 16.04

firefox\_50.1.0+build2-0ubuntu0.16.04.1

Ubuntu 14.04

firefox\_50.1.0+build2-0ubuntu0.14.04.1

Ubuntu 16.10

firefox\_50.1.0+build2-0ubuntu0.16.10.1

## 185521 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3156-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1252

### Description

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

USN-3156-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-December/003669.html>

Ubuntu 16.04

apt\_1.2.15ubuntu0.2

Ubuntu 14.04

apt\_1.0.1ubuntu2.17

Ubuntu 16.10

apt\_1.3.2ubuntu0.1

#### 191456 - Fedora Linux 23 FEDORA-2016-7fc142da66 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4412

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-7fc142da66

##### 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/2016/12/?count=200&page=3>

Fedora Core 23

phpMyAdmin-4.6.5.1-2.fc23

#### 191457 - Fedora Linux 24 FEDORA-2016-2460f713a1 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-2016-2460f713a1

##### 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/2016/12/?count=200&page=3>

Fedora Core 24

php-php-gettext-1.0.12-1.fc24

#### 191458 - Fedora Linux 25 FEDORA-2016-9c63b652a8 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9809, CVE-2016-9812, CVE-2016-9813

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-9c63b652a8



### 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/2016/12/?count=200&page=3>

Fedora Core 25

gstreamer-plugins-bad-free-0.10.23-35.fc25

### **191459 - Fedora Linux 25 FEDORA-2016-a1563af431 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-2016-a1563af431

### 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/2016/12/?count=200&page=1>

Fedora Core 25

golang-1.7.4-1.fc25

### **191461 - Fedora Linux 25 FEDORA-2016-868350fe5a Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8649

### Description

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

FEDORA-2016-868350fe5a

### 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/2016/12/?count=200&page=1>

Fedora Core 25

lxc-2.0.6-2.fc25

### **191462 - Fedora Linux 24 FEDORA-2016-c198d15316 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-c198d15316

#### 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/2016/12/?count=200&page=3>

Fedora Core 24

ntp-4.2.6p5-43.fc24

### **191463 - Fedora Linux 24 FEDORA-2016-b4dd1db1e7 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8649

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-b4dd1db1e7

#### 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/2016/12/?count=200&page=1>

Fedora Core 24

lxc-2.0.6-2.fc24

### **191464 - Fedora Linux 25 FEDORA-2016-bbe98c341c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9755, CVE-2016-9756, CVE-2016-9777

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-bbe98c341c

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

kernel-4.8.12-300.fc25

### 191465 - Fedora Linux 24 FEDORA-2016-fad6fc78dd 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-2016-fad6fc78dd

#### 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/2016/12/?count=200&page=1>

Fedora Core 24

golang-1.6.4-2.fc24

### 191466 - Fedora Linux 23 FEDORA-2016-7da97a3914 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-2016-7da97a3914

#### 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/2016/12/?count=200&page=2>

Fedora Core 23

mcabber-1.0.4-1.fc23

### 191467 - Fedora Linux 25 FEDORA-2016-7209ab4e02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-7209ab4e02

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

ntp-4.2.6p5-43.fc25

#### **191468 - Fedora Linux 25 FEDORA-2016-dcde4f3cd2 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636, CVE-2016-9808

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-dcde4f3cd2

##### 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/2016/12/?count=200&page=3>

Fedora Core 25

gststreamer-plugins-good-0.10.31-17.fc25

#### **191469 - Fedora Linux 24 FEDORA-2016-a17657197c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9811

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-a17657197c

##### 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/2016/12/?count=200&page=2>

Fedora Core 24

gststreamer-plugins-base-0.10.36-15.fc24

#### **191470 - Fedora Linux 24 FEDORA-2016-a3618d9ef6 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-2016-a3618d9ef6

## 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/2016/12/?count=200&page=1>

Fedora Core 24

python-tornado-4.4.2-1.fc24

### **191472 - Fedora Linux 24 FEDORA-2016-4fff0cbc66 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9811

## Description

The scan detected that the host is missing the following update:  
FEDORA-2016-4fff0cbc66

## 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/2016/12/?count=200&page=3>

Fedora Core 24

gststreamer1-plugins-base-1.8.3-2.fc24

### **191473 - Fedora Linux 25 FEDORA-2016-fc8577bf00 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9572, CVE-2016-9573

## Description

The scan detected that the host is missing the following update:  
FEDORA-2016-fc8577bf00

## 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/2016/12/?count=200&page=3>

Fedora Core 25

openjpeg2-2.1.2-2.fc25

### 191474 - Fedora Linux 25 FEDORA-2016-4c8140241f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9811

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-4c8140241f

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

gstreamer-plugins-base-0.10.36-15.fc25

### 191475 - Fedora Linux 23 FEDORA-2016-a571b97ebb 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-2016-a571b97ebb

#### 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/2016/12/?count=200&page=3>

Fedora Core 23

php-php-gettext-1.0.12-1.fc23

### 191476 - Fedora Linux 24 FEDORA-2016-2424eeca35 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4412

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-2424eeca35

#### 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/2016/12/?count=200&page=3>

Fedora Core 24

phpMyAdmin-4.6.5.1-2.fc24

### 191478 - Fedora Linux 24 FEDORA-2016-0b80dcfe5a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9572, CVE-2016-9573

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-0b80dcfe5a

#### 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/2016/12/?count=200&page=2>

Fedora Core 24

openjpeg2-2.1.2-2.fc24

### 191480 - Fedora Linux 23 FEDORA-2016-637618fcd4 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-2016-637618fcd4

#### 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/2016/12/?count=200&page=4>

Fedora Core 23

mingw-nsis-2.50-1.fc23

### 191481 - Fedora Linux 24 FEDORA-2016-ca6cc3ce3e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9809, CVE-2016-9812, CVE-2016-9813

#### Description

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

FEDORA-2016-ca6cc3ce3e

#### 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/2016/12/?count=200&page=3>

Fedora Core 24

gstreamer1-plugins-bad-free-1.8.3-3.fc24

### **191484 - Fedora Linux 25 FEDORA-2016-e865601498 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-2016-e865601498

#### 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/2016/12/?count=200&page=2>

Fedora Core 25

mcabber-1.0.4-1.fc25

### **191485 - Fedora Linux 25 FEDORA-2016-077d0ed22e 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-2016-077d0ed22e

#### 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/2016/12/?count=200&page=3>

Fedora Core 25

php-php-gettext-1.0.12-1.fc25

### **191486 - Fedora Linux 24 FEDORA-2016-b000091725 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-2016-b000091725

#### 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/2016/12/?count=200&page=1>

Fedora Core 24

php-simplesamlphp-saml2-2.3.3-1.fc24  
php-simplesamlphp-saml2\_1-1.10.3-1.fc24

### **191488 - Fedora Linux 23 FEDORA-2016-5c32bae671 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-2016-5c32bae671

#### 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/2016/12/?count=200&page=1>

Fedora Core 23

php-simplesamlphp-saml2\_1-1.10.3-1.fc23  
php-simplesamlphp-saml2-2.3.3-1.fc23

### **191489 - Fedora Linux 25 FEDORA-2016-8b1f72df21 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-2016-8b1f72df21

#### 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/2016/12/?count=200&page=1>

Fedora Core 25

php-simplesamlphp-saml2\_1-1.10.3-1.fc25

php-simplesamlphp-saml2-2.3.3-1.fc25

#### 191490 - Fedora Linux 24 FEDORA-2016-30f68ec06b 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-2016-30f68ec06b

##### 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/2016/12/?count=200&page=2>

Fedora Core 24

mcabber-1.0.4-1.fc24

#### 191491 - Fedora Linux 25 FEDORA-2016-dd2aa2b4a9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8687, CVE-2016-8688, CVE-2016-8689

##### Description

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

FEDORA-2016-dd2aa2b4a9

##### 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/2016/12/?count=200&page=2>

Fedora Core 25

mingw-libarchive-3.2.2-1.fc25

#### 191495 - Fedora Linux 23 FEDORA-2016-9c17cb9648 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9755, CVE-2016-9756, CVE-2016-9777

##### Description

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

FEDORA-2016-9c17cb9648

### 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/2016/12/?count=200&page=3>

Fedora Core 23

kernel-4.8.12-100.fc23

### **191496 - Fedora Linux 23 FEDORA-2016-e8a8561ee7 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-e8a8561ee7

### 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/2016/12/?count=200&page=3>

Fedora Core 23

ntp-4.2.6p5-43.fc23

### **191498 - Fedora Linux 25 FEDORA-2016-0c4e822340 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-0c4e822340

### 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/2016/12/?count=200&page=3>

Fedora Core 25

memcached-1.4.33-1.fc25

### **191499 - Fedora Linux 24 FEDORA-2016-5ec2475e3f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9755, CVE-2016-9756, CVE-2016-9777

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-5ec2475e3f

#### 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/2016/12/?count=200&page=3>

Fedora Core 24

kernel-4.8.12-200.fc24

### 178273 - Gentoo Linux GLSA-201612-28 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3697

#### Description

The scan detected that the host is missing the following update:  
GLSA-201612-28

#### Observation

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

<https://security.gentoo.org/glsa/201612-28>

Affected packages:

app-emulation/docker < 1.11.0

## 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.

### 5844 - Apple QuickTime Crafted MOV File Code Execution

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

Risk Level: High

CVE: CVE-2008-2010

#### Update Details

Recommendation is updated

### 6139 - Apple Quicktime Stack\_Cookie Stack Overflow Vulnerability

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4116

[Update Details](#)

Recommendation is updated

### 9667 - Allied Telesyn TFTP Server Long Filename Remote Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2006-6184

[Update Details](#)

Recommendation is updated

### 10061 - Atrium Mercur Messaging IMAP Service Remote Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2006-1255

[Update Details](#)

Recommendation is updated

### 14527 - Adobe Flash Player FLV File Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

### 14539 - Adobe Shockwave Player Multiple Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-2012-6270, CVE-2012-6271

[Update Details](#)

Recommendation is updated

### 18061 - Avinu phpMoAdmin saveObject Unauthorized Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-2208

[Update Details](#)

Recommendation is updated

**18234 - ANT Studio Web DLL Hijacking Remote Code Execution**

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

**38132 - Apple QuickTime Crafted MOV File Code Execution**

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

Risk Level: High

CVE: CVE-2008-2010

[Update Details](#)

Recommendation is updated

**38159 - Apple Quicktime Stack\_Cookie Stack Overflow Vulnerability**

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

Risk Level: High

CVE: CVE-2008-4116

[Update Details](#)

Recommendation is updated

**13053 - Adobe Flash Player VulnDisco Step Ahead Remote Code Execution**

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

Risk Level: High

CVE: CVE-2011-4693, CVE-2011-4694

[Update Details](#)

Recommendation is updated

**13123 - AVID Media Composer Phonetic Indexer Stack Buffer Overflow Remote Code Execution**

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

Risk Level: High

CVE: CVE-2011-5003

[Update Details](#)

Recommendation is updated

### 3823 - Alt-N MDAemon Local Privilege Escalation

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

Risk Level: High

CVE: CVE-2004-2504

#### [Update Details](#)

Recommendation is updated

### 12852 - A-Blog Sources Search.php SQL Injection Remote Code Execution

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

Risk Level: High

CVE: CVE-2010-4917

#### [Update Details](#)

Recommendation is updated

### 12951 - Apple OS X Sandbox Predefined Profiles Bypass Remote Code Execution II

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

Risk Level: High

CVE: CVE-2008-7303

#### [Update Details](#)

Recommendation is updated

### 12952 - Apple OS X Sandbox Predefined Profiles Bypass Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-1516

#### [Update Details](#)

Recommendation is updated

### 13435 - Apple Safari Plug-in Unloading Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-3845

#### [Update Details](#)

Recommendation is updated

### 20103 - Autodesk Backburner Manager Stack Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2016-2344

[Update Details](#)

Recommendation is updated

**88817 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-305-02 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5407, CVE-2016-7942, CVE-2016-7943, CVE-2016-7944, CVE-2016-7945, CVE-2016-7946, CVE-2016-7947, CVE-2016-7948, CVE-2016-7949, CVE-2016-7950, CVE-2016-7951, CVE-2016-7952, CVE-2016-7953

[Update Details](#)

Risk is updated

**182156 - FreeBSD django Multiple Vulnerabilities (cb116651-79db-4c09-93a2-c38f9df46724)**

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

Risk Level: High

CVE: CVE-2016-9013, CVE-2016-9014

[Update Details](#)

Risk is updated

**185466 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3115-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-9013, CVE-2016-9014

[Update Details](#)

Risk is updated

**191205 - Fedora Linux 25 FEDORA-2016-ade20198ff Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7949, CVE-2016-7950

[Update Details](#)

Risk is updated

**191211 - Fedora Linux 25 FEDORA-2016-a06c8cc941 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7947, CVE-2016-7948

[Update Details](#)

Risk is updated



**191222 - Fedora Linux 25 FEDORA-2016-37b9932690 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7953

Update Details

Risk is updated

**191229 - Fedora Linux 24 FEDORA-2016-a236cb3315 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7953

Update Details

Risk is updated

**191236 - Fedora Linux 24 FEDORA-2016-83040426d6 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7947, CVE-2016-7948

Update Details

Risk is updated

**191243 - Fedora Linux 25 FEDORA-2016-e6ba110670 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7951, CVE-2016-7952

Update Details

Risk is updated

**191244 - Fedora Linux 24 FEDORA-2016-8877cf648b Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7949, CVE-2016-7950

Update Details

Risk is updated

**191247 - Fedora Linux 24 FEDORA-2016-c1d4b1df79 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7951, CVE-2016-7952

[Update Details](#)

Risk is updated

**191249 - Fedora Linux 25 FEDORA-2016-0df69ab477 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7942, CVE-2016-7943

[Update Details](#)

Risk is updated

**191253 - Fedora Linux 24 FEDORA-2016-ff5a2f4839 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7944

[Update Details](#)

Risk is updated

**191259 - Fedora Linux 25 FEDORA-2016-72d7f05b90 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7944

[Update Details](#)

Risk is updated

**191312 - Fedora Linux 23 FEDORA-2016-0e7694c456 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7944

[Update Details](#)

Risk is updated

**191314 - Fedora Linux 23 FEDORA-2016-d286ffb801 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7953

[Update Details](#)

Risk is updated

**191315 - Fedora Linux 23 FEDORA-2016-49d560da23 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7949, CVE-2016-7950

[Update Details](#)

Risk is updated

#### 191325 - Fedora Linux 23 FEDORA-2016-b26b497381 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7951, CVE-2016-7952

[Update Details](#)

Risk is updated

#### 191326 - Fedora Linux 23 FEDORA-2016-d045c2c7b3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7947, CVE-2016-7948

[Update Details](#)

Risk is updated

#### 191346 - Fedora Linux 24 FEDORA-2016-3eb5a55123 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9013, CVE-2016-9014

[Update Details](#)

Risk is updated

#### 191366 - Fedora Linux 25 FEDORA-2016-d4571bf555 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9013, CVE-2016-9014

[Update Details](#)

Risk is updated

#### 845 - Apache Win32 PHP.EXE Remote File Disclosure

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

Risk Level: Medium

CVE: CVE-2002-2029

[Update Details](#)

Recommendation is updated

---

### 937 - Apple Airport Base Station WEP Key Disclosure

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Update Details

Recommendation is updated

### 6980 - Apache HTTPD suexec Multiple Local Privilege Escalation Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2007-1741, CVE-2007-1742, CVE-2007-1743

#### Update Details

Recommendation is updated

### 12963 - Adobe ColdFusion Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

#### Update Details

Recommendation is updated

### 130560 - Debian Linux 8.0 DSA-3646-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### 141270 - Red Hat Enterprise Linux RHSA-2016-1781 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### 141274 - Red Hat Enterprise Linux RHSA-2016-1820 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

**141275 - Red Hat Enterprise Linux RHSA-2016-1821 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

**141335 - Red Hat Enterprise Linux RHSA-2016-2606 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

**144796 - SuSE Linux 13.2 openSUSE-SU-2016:2072-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5010, CVE-2016-6491, CVE-2016-6520

[Update Details](#)

Risk is updated

**144800 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2076-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5010, CVE-2016-6491, CVE-2016-6520

[Update Details](#)

Risk is updated

**144801 - SuSE SLES 11 SP4 SUSE-SU-2016:2075-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6491, CVE-2016-6520

[Update Details](#)

Risk is updated

**144897 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2415-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

#### **144898 - SuSE Linux 13.2 openSUSE-SU-2016:2425-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

#### **144903 - SuSE SLES 11 SP4 SUSE-SU-2016:2418-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

#### **163188 - Oracle Enterprise Linux ELSA-2016-2606 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

#### **170720 - Amazon Linux AMI ALAS-2016-747 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

#### **182089 - FreeBSD PostgreSQL Denial-of-Service And Code Injection Vulnerabilities (ca16fd0b-5fd1-11e6-a6f2-6cc21735f730)**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

[Update Details](#)

Risk is updated

### **185391 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3066-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### **191019 - Fedora Linux 24 FEDORA-2016-30b01bdeed Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### **191020 - Fedora Linux 23 FEDORA-2016-5486a6dfc0 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### **191053 - Fedora Linux 25 FEDORA-2016-765bb26915 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5423, CVE-2016-5424

#### Update Details

Risk is updated

### **1855 - Apache mod\_access\_referer NULL Pointer Denial of Service**

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

Risk Level: Medium

CVE: CVE-2003-1054

#### Update Details

Recommendation is updated

### **4307 - Armada Master Index search.cgi Directory Traversal**

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

Risk Level: Medium

CVE: CVE-2000-0924

[Update Details](#)

Recommendation is updated

### 8129 - Apache HTTP Server mod\_rewrite Security Bypass Vulnerability

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

Risk Level: Medium

CVE: CVE-2001-1072

[Update Details](#)

Recommendation is updated

### 9828 - Apple Mac OS X WebDAV Kernel Extension Denial Of Service (CVE-2010-1794)

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

Risk Level: Medium

CVE: CVE-2010-1794

[Update Details](#)

Recommendation is updated

### 14508 - Apache Tomcat Slowloris HTTP Denial of Service

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

Risk Level: Medium

CVE: CVE-2012-5568

[Update Details](#)

Recommendation is updated

### 14676 - Apple QuickTime Out of Bound Read Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

### 17037 - Advantech Domain Focused Configuration Tool Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated



### 19545 - Intel McAfee ePolicy Orchestrator Apache Commons Remote Code Execution

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

Risk Level: Medium

CVE: CVE-2015-8765

#### Update Details

FASLScript is updated

### 20567 - (SOL05016441) F5 BIG-IP Oracle Java Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-3508

#### Update Details

Recommendation is updated

### 130617 - Debian Linux 8.0 DSA-3702-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6321

#### Update Details

Risk is updated

### 145014 - SuSE Linux 13.2 openSUSE-SU-2016:2874-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6321

#### Update Details

Risk is updated

### 145024 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2896-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6321

#### Update Details

Risk is updated

### 145025 - SuSE SLES 11 SP4 SUSE-SU-2016:2895-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6321

[Update Details](#)

Risk is updated

**185487 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3132-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6321

[Update Details](#)

Risk is updated

**191241 - Fedora Linux 24 FEDORA-2016-cabb6d7ef7 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7945, CVE-2016-7946

[Update Details](#)

Risk is updated

**191248 - Fedora Linux 25 FEDORA-2016-8b122b0997 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7945, CVE-2016-7946

[Update Details](#)

Risk is updated

**191357 - Fedora Linux 23 FEDORA-2016-21f0de504c Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7945, CVE-2016-7946

[Update Details](#)

Risk is updated

**9153 - Apache HTTP Server mod\_alias URL Validation Canonicalization CGI Script Source Code Disclosure Vulnerability**

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

Risk Level: Medium

CVE: CVE-2006-4110

[Update Details](#)

Recommendation is updated

**19586 - (SOL02360853) F5 BIG-IP NTP Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-5194, CVE-2015-5195

[Update Details](#)

Recommendation is updated

**20620 - (SOL01324833) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2015-8158

[Update Details](#)

Recommendation is updated

**33178 - Oracle Solaris 137204-38 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

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

**33180 - Oracle Solaris 137205-38 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

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

**8083 - Apache HTTP Server OS Fingerprinting Vulnerability**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

**70074 - mcafee.fasl3.inc**

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

---

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Update Details

FASLScript is updated

## HOW TO UPDATE

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

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

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

## MCAFFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

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

Copyright 2016 McAfee, Inc.

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