

## 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

#### 22333 - (K41103561) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-4448

#### Description

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

#### Observation

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

A format string vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in libxml2. Successful exploitation could allow an attacker unauthorized disclosure of information, unauthorized modification, and disruption of service.

#### 132393 - Oracle VM OVMSA-2017-0145 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10200, CVE-2016-10208, CVE-2016-10229, CVE-2016-1575, CVE-2016-1576, CVE-2016-6213, CVE-2016-7910, CVE-2016-8399, CVE-2016-9604, CVE-2016-9644, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-2583, CVE-2017-2636, CVE-2017-2671, CVE-2017-5669, CVE-2017-5986, CVE-2017-6214, CVE-2017-6345, CVE-2017-6347, CVE-2017-7184, CVE-2017-7187, CVE-2017-7273, CVE-2017-7308, CVE-2017-7477, CVE-2017-7533, CVE-2017-7645, CVE-2017-7895, CVE-2017-8797, CVE-2017-8890, CVE-2017-9059, CVE-2017-9074, CVE-2017-9077, CVE-2017-9242

#### Description

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

OVMSA-2017-0145

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000760.html>

OVM3.4

x86\_64

kernel-uek-4.1.12-103.3.8.el6uek

kernel-uek-firmware-4.1.12-103.3.8.el6uek

#### 132394 - Oracle VM OVMSA-2017-0142 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9603, CVE-2017-10912, CVE-2017-10913, CVE-2017-10914, CVE-2017-10915, CVE-2017-10917, CVE-2017-10918, CVE-2017-10920, CVE-2017-10921, CVE-2017-10922, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-2615, CVE-2017-2620, CVE-2017-7228, CVE-2017-8903, CVE-2017-8904, CVE-2017-8905

#### Description

The scan detected that the host is missing the following update:  
OVMSA-2017-0142

#### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2017-August/000772.html>

OVM3.4  
x86\_64  
xen-4.4.4-155.el6  
xen-tools-4.4.4-155.el6

### 163447 - Oracle Enterprise Linux ELSA-2017-3609 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10200, CVE-2016-10208, CVE-2016-10229, CVE-2016-1575, CVE-2016-1576, CVE-2016-6213, CVE-2016-7910, CVE-2016-8399, CVE-2016-9604, CVE-2016-9644, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-12134, CVE-2017-2583, CVE-2017-2636, CVE-2017-2671, CVE-2017-5669, CVE-2017-5986, CVE-2017-6214, CVE-2017-6345, CVE-2017-6347, CVE-2017-7184, CVE-2017-7187, CVE-2017-7273, CVE-2017-7308, CVE-2017-7477, CVE-2017-7533, CVE-2017-7645, CVE-2017-7895, CVE-2017-8797, CVE-2017-8890, CVE-2017-9059, CVE-2017-9074, CVE-2017-9077, CVE-2017-9242

#### Description

The scan detected that the host is missing the following update:  
ELSA-2017-3609

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-August/007157.html>  
<http://oss.oracle.com/pipermail/el-errata/2017-August/007158.html>

OEL7  
x86\_64  
kernel-uek-firmware-4.1.12-103.3.8.el7uek  
dtrace-modules-shared-headers-0.6.1-3.el7  
kernel-uek-debug-4.1.12-103.3.8.el7uek  
dtrace-modules-provider-headers-0.6.1-3.el7  
kernel-uek-4.1.12-103.3.8.el7uek  
kernel-uek-devel-4.1.12-103.3.8.el7uek  
kernel-uek-doc-4.1.12-103.3.8.el7uek  
kernel-uek-debug-devel-4.1.12-103.3.8.el7uek  
dtrace-modules-4.1.12-103.3.8.el7uek-0.6.1-3.el7

OEL6

x86\_64  
kernel-uek-debug-4.1.12-103.3.8.el6uek  
dtrace-modules-4.1.12-103.3.8.el6uek-0.6.1-3.el6  
kernel-uek-doc-4.1.12-103.3.8.el6uek  
kernel-uek-devel-4.1.12-103.3.8.el6uek  
kernel-uek-4.1.12-103.3.8.el6uek  
kernel-uek-debug-devel-4.1.12-103.3.8.el6uek  
dtrace-modules-provider-headers-0.6.1-3.el6  
dtrace-modules-shared-headers-0.6.1-3.el6  
kernel-uek-firmware-4.1.12-103.3.8.el6uek

## 185860 - Ubuntu Linux 14.04 USN-3405-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7837, CVE-2017-11176, CVE-2017-7495, CVE-2017-7541

### Description

The scan detected that the host is missing the following update:  
USN-3405-2

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004029.html>

Ubuntu 14.04

linux-image-4.4.0-93-powerpc-e500mc\_4.4.0-93.116~14.04.1  
linux-image-powerpc64-smp-lts-xenial\_4.4.0.93.77  
linux-image-4.4.0-93-lowlatency\_4.4.0-93.116~14.04.1  
linux-image-4.4.0-93-powerpc64-emb\_4.4.0-93.116~14.04.1  
linux-image-4.4.0-93-generic-lpae\_4.4.0-93.116~14.04.1  
linux-image-powerpc64-emb-lts-xenial\_4.4.0.93.77  
linux-image-powerpc-e500mc-lts-xenial\_4.4.0.93.77  
linux-image-4.4.0-93-generic\_4.4.0-93.116~14.04.1  
linux-image-powerpc-smp-lts-xenial\_4.4.0.93.77  
linux-image-generic-lpae-lts-xenial\_4.4.0.93.77  
linux-image-4.4.0-93-powerpc64-smp\_4.4.0-93.116~14.04.1  
linux-image-generic-lts-xenial\_4.4.0.93.77  
linux-image-lowlatency-lts-xenial\_4.4.0.93.77  
linux-image-4.4.0-93-powerpc-smp\_4.4.0-93.116~14.04.1

## 185862 - Ubuntu Linux 16.04 USN-3405-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7837, CVE-2017-11176, CVE-2017-7495, CVE-2017-7541

### Description

The scan detected that the host is missing the following update:  
USN-3405-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004028.html>

Ubuntu 16.04

linux-image-powerpc64-emb\_4.4.0.93.98  
linux-image-aws\_4.4.0.1032.34  
linux-image-4.4.0-93-powerpc-smp\_4.4.0-93.116  
linux-image-4.4.0-1071-raspi2\_4.4.0-1071.79  
linux-image-powerpc-smp\_4.4.0.93.98  
linux-image-4.4.0-93-powerpc-e500mc\_4.4.0-93.116  
linux-image-gke\_4.4.0.1028.29  
linux-image-generic\_4.4.0.93.98  
linux-image-4.4.0-1073-snapdragon\_4.4.0-1073.78  
linux-image-generic-lpae\_4.4.0.93.98  
linux-image-4.4.0-93-lowlatency\_4.4.0-93.116  
linux-image-4.4.0-93-powerpc64-emb\_4.4.0-93.116  
linux-image-lowlatency\_4.4.0.93.98  
linux-image-raspi2\_4.4.0.1071.71  
linux-image-4.4.0-1032-aws\_4.4.0-1032.41  
linux-image-4.4.0-93-generic-lpae\_4.4.0-93.116  
linux-image-4.4.0-93-powerpc64-smp\_4.4.0-93.116  
linux-image-powerpc64-smp\_4.4.0.93.98  
linux-image-snapdragon\_4.4.0.1073.65  
linux-image-4.4.0-93-generic\_4.4.0-93.116  
linux-image-4.4.0-1028-gke\_4.4.0-1028.28

### 22314 - (K21154730) F5 BIG-IP TMM SSL/TLS Profile Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6141

#### Description

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

#### Observation

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

A denial of service is present in some versions of F5 BIG-IP systems. The flaw lies in the Traffic Management Microkernel (TMM) when a client SSL profile has the Session Ticket option enabled. Successful exploitation could allow a remote attacker to cause a denial of service condition.

### 22329 - IBM AIX Bind Multiple Vulnerabilities (bind\_advisory16.asc)

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

Risk Level: High

CVE: CVE-2017-3142, CVE-2017-3143

#### Description

Multiple vulnerabilities are present in some versions of IBM AIX.

#### Observation

IBM AIX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in BIND. Successful exploitation could allow an attacker to bypass TSIG authentication.

### 22247 - Google Chrome Multiple Vulnerabilities Prior To 60.0.3112.78

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

Risk Level: High

CVE: CVE-2017-5091, CVE-2017-5092, CVE-2017-5093, CVE-2017-5094, CVE-2017-5095, CVE-2017-5096, CVE-2017-5097, CVE-2017-5098, CVE-2017-5099, CVE-2017-5100, CVE-2017-5101, CVE-2017-5102, CVE-2017-5103, CVE-2017-5104, CVE-2017-5105, CVE-2017-5106, CVE-2017-5107, CVE-2017-5108, CVE-2017-5109, CVE-2017-5110, CVE-2017-6991

#### 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 multiple component. Successful exploitation allow an attacker to conduct spoofing attacks or retrieve sensitive data.

### 22248 - Google Chrome Multiple Vulnerabilities Prior To 60.0.3112.78

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5091, CVE-2017-5092, CVE-2017-5093, CVE-2017-5094, CVE-2017-5095, CVE-2017-5096, CVE-2017-5097, CVE-2017-5098, CVE-2017-5099, CVE-2017-5100, CVE-2017-5101, CVE-2017-5102, CVE-2017-5103, CVE-2017-5104, CVE-2017-5105, CVE-2017-5106, CVE-2017-5107, CVE-2017-5108, CVE-2017-5109, CVE-2017-5110, CVE-2017-6991

#### 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 multiple component. Successful exploitation allow an attacker to conduct spoofing attacks or retrieve sensitive data.

### 22320 - Splunk Enterprise Multiple Vulnerabilities (SP-CAAAP3H)

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

#### Description

Multiple XSS vulnerabilities are present in some versions of Splunk Enterprise.

#### Observation

Splunk Enterprise is a platform for real-time operational intelligence.

Multiple XSS vulnerabilities are present in some versions of Splunk Enterprise. The flaw lies in all components running Splunk Web. Successful exploitation could allow an attacker to execute arbitrary code.

## 22325 - (K43267483) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-5766

### Description

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

### Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in PHP. Successful exploitation could allow an attacker to cause a denial of service condition or have unspecified other impact.

## 22339 - SpiderControl SCADA MicroBrowser Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2017-12707

### Description

A stack-based buffer overflow vulnerability is present in some versions of SpiderControl Scada MicroBrowser.

### Observation

The SpiderControl MicroBrowser is a Viewer for HMI's designed with SpiderControl Editor.

A stack-based buffer overflow vulnerability is present in some versions of SpiderControl Scada MicroBrowser. The flaw is due to lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. Successful exploitation by a remote attacker could result in the execution of arbitrary code, the exploit requires the user to open a malicious website or open a malicious file. Failed attempts will result in a denial of service condition.

## 130861 - Debian Linux 8.0 DSA-3951-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8849

### Description

The scan detected that the host is missing the following update:  
DSA-3951-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3951>

Debian 8.0  
all  
smb4k\_1.2.1-2~deb8u1

## 141695 - Red Hat Enterprise Linux RHSA-2017-2534 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

### Description

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

RHSA-2017-2534

### Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00077.html>

#### RHEL7S

x86\_64

thunderbird-debuginfo-52.3.0-1.el7\_4

thunderbird-52.3.0-1.el7\_4

#### RHEL6S

i386

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

x86\_64

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

#### RHEL6WS

x86\_64

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

i386

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

#### RHEL7D

x86\_64

thunderbird-debuginfo-52.3.0-1.el7\_4

thunderbird-52.3.0-1.el7\_4

#### RHEL6D

x86\_64

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

i386

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

#### RHEL7WS

x86\_64

thunderbird-debuginfo-52.3.0-1.el7\_4

thunderbird-52.3.0-1.el7\_4

## 145496 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2286-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-10810, CVE-2017-11473, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-8831

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2286-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003165.html>

SuSE SLED 12 SP3

x86\_64

kernel-default-4.4.82-6.3.1

kernel-default-extra-debuginfo-4.4.82-6.3.1

kernel-default-debuginfo-4.4.82-6.3.1

kernel-default-debugsource-4.4.82-6.3.1

kernel-default-extra-4.4.82-6.3.1

kernel-default-devel-4.4.82-6.3.1

kernel-syms-4.4.82-6.3.1

noarch

kernel-devel-4.4.82-6.3.1

kernel-macros-4.4.82-6.3.1

kernel-source-4.4.82-6.3.1

SuSE SLES 12 SP3

noarch

kernel-devel-4.4.82-6.3.1

kernel-macros-4.4.82-6.3.1

kernel-source-4.4.82-6.3.1

x86\_64

kernel-default-4.4.82-6.3.1

kernel-default-base-4.4.82-6.3.1

kernel-default-base-debuginfo-4.4.82-6.3.1

kernel-default-debuginfo-4.4.82-6.3.1

kernel-default-debugsource-4.4.82-6.3.1

kernel-default-devel-4.4.82-6.3.1

kernel-syms-4.4.82-6.3.1

## 145498 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2017:2264-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7435, CVE-2017-7436, CVE-2017-9269

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2264-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003160.html>

SuSE SLED 12 SP3

x86\_64

yast2-pkg-bindings-debugsource-3.2.4-2.3.1

yast2-pkg-bindings-debuginfo-3.2.4-2.3.1

libzypp-debuginfo-16.15.3-2.3.1

libzypp-debugsource-16.15.3-2.3.1

yast2-pkg-bindings-3.2.4-2.3.1

libzypp-16.15.3-2.3.1

SuSE SLES 12 SP3

x86\_64

yast2-pkg-bindings-debugsource-3.2.4-2.3.1

yast2-pkg-bindings-debuginfo-3.2.4-2.3.1

libzypp-debuginfo-16.15.3-2.3.1

libzypp-debugsource-16.15.3-2.3.1

yast2-pkg-bindings-3.2.4-2.3.1

libzypp-16.15.3-2.3.1

## **145499 - SuSE SLES 12 SP2 SUSE-SU-2017:2243-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10987, CVE-2017-10988

## Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2243-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003153.html>

SuSE SLES 12 SP2

x86\_64

freeradius-server-libs-debuginfo-3.0.3-17.9.1

freeradius-server-doc-3.0.3-17.9.1

freeradius-server-mysql-debuginfo-3.0.3-17.9.1

freeradius-server-sqlite-debuginfo-3.0.3-17.9.1

freeradius-server-perl-3.0.3-17.9.1

freeradius-server-python-3.0.3-17.9.1

freeradius-server-3.0.3-17.9.1

freeradius-server-postgresql-debuginfo-3.0.3-17.9.1

freeradius-server-perl-debuginfo-3.0.3-17.9.1

freeradius-server-ldap-debuginfo-3.0.3-17.9.1

freeradius-server-krb5-3.0.3-17.9.1

freeradius-server-postgresql-3.0.3-17.9.1

freeradius-server-sqlite-3.0.3-17.9.1

freeradius-server-utils-debuginfo-3.0.3-17.9.1

freeradius-server-mysql-3.0.3-17.9.1

freeradius-server-utils-3.0.3-17.9.1  
freeradius-server-debuginfo-3.0.3-17.9.1  
freeradius-server-python-debuginfo-3.0.3-17.9.1  
freeradius-server-krb5-debuginfo-3.0.3-17.9.1  
freeradius-server-debugsource-3.0.3-17.9.1  
freeradius-server-libs-3.0.3-17.9.1  
freeradius-server-ldap-3.0.3-17.9.1

### 145500 - SuSE SLES 11 SP4 SUSE-SU-2017:2244-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10979, CVE-2017-10981, CVE-2017-10982, CVE-2017-10983

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2244-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003154.html>

SuSE SLES 11 SP4

i586

freeradius-server-doc-2.1.1-7.25.3.1  
freeradius-server-utils-2.1.1-7.25.3.1  
freeradius-server-dialupadmin-2.1.1-7.25.3.1  
freeradius-server-2.1.1-7.25.3.1  
freeradius-server-libs-2.1.1-7.25.3.1

x86\_64

freeradius-server-doc-2.1.1-7.25.3.1  
freeradius-server-utils-2.1.1-7.25.3.1  
freeradius-server-dialupadmin-2.1.1-7.25.3.1  
freeradius-server-2.1.1-7.25.3.1  
freeradius-server-libs-2.1.1-7.25.3.1

### 145501 - SuSE SLES 11 SP4 SUSE-SU-2017:2258-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2258-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003158.html>

SuSE SLES 11 SP4

i586  
postgresql94-9.4.13-0.23.5.1  
libecpg6-9.4.13-0.23.5.1  
libpq5-9.4.13-0.23.5.1  
postgresql94-docs-9.4.13-0.23.5.1  
postgresql94-contrib-9.4.13-0.23.5.1  
postgresql94-server-9.4.13-0.23.5.1

x86\_64  
postgresql94-9.4.13-0.23.5.1  
libecpg6-9.4.13-0.23.5.1  
libpq5-9.4.13-0.23.5.1  
postgresql94-docs-9.4.13-0.23.5.1  
postgresql94-contrib-9.4.13-0.23.5.1  
postgresql94-server-9.4.13-0.23.5.1  
libpq5-32bit-9.4.13-0.23.5.1

## 145503 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2294-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1245, CVE-2017-5495

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2294-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003168.html>

### SuSE SLES 12 SP3

x86\_64  
quagga-debuginfo-1.1.1-17.3.3  
libquagga\_pb0-debuginfo-1.1.1-17.3.3  
quagga-1.1.1-17.3.3  
libospfapiclient0-1.1.1-17.3.3  
libfpm\_pb0-debuginfo-1.1.1-17.3.3  
libzebra1-debuginfo-1.1.1-17.3.3  
libospf0-debuginfo-1.1.1-17.3.3  
quagga-debugsource-1.1.1-17.3.3  
libzebra1-1.1.1-17.3.3  
libospfapiclient0-debuginfo-1.1.1-17.3.3  
libfpm\_pb0-1.1.1-17.3.3  
libospf0-1.1.1-17.3.3  
libquagga\_pb0-1.1.1-17.3.3

### SuSE SLES 12 SP2

x86\_64  
quagga-debuginfo-1.1.1-17.3.3  
libquagga\_pb0-debuginfo-1.1.1-17.3.3  
quagga-1.1.1-17.3.3  
libospfapiclient0-1.1.1-17.3.3  
libfpm\_pb0-debuginfo-1.1.1-17.3.3  
libzebra1-debuginfo-1.1.1-17.3.3  
libospf0-debuginfo-1.1.1-17.3.3

quagga-debugsource-1.1.1-17.3.3  
libzebra1-1.1.1-17.3.3  
libospfapiclient0-debuginfo-1.1.1-17.3.3  
libfpm\_pb0-1.1.1-17.3.3  
libospf0-1.1.1-17.3.3  
libquagga\_pb0-1.1.1-17.3.3

## 163448 - Oracle Enterprise Linux ELSA-2017-2534 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

### Description

The scan detected that the host is missing the following update:  
ELSA-2017-2534

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-August/007162.html>  
<http://oss.oracle.com/pipermail/el-errata/2017-August/007163.html>

OEL7  
x86\_64  
thunderbird-52.3.0-1.0.1.el7\_4

OEL6  
x86\_64  
thunderbird-52.3.0-1.0.1.el6\_9

i386  
thunderbird-52.3.0-1.0.1.el6\_9

## 175252 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86\_64 (1708-23241)

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

Risk Level: High

CVE: CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: thunderbird on SL6.x, SL7.x i386/x86\_64 (1708-23241)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1708&L=scientific-linux-errata&F=&S=&P=23241>

SL7  
x86\_64  
thunderbird-debuginfo-52.3.0-1.el7\_4

thunderbird-52.3.0-1.el7\_4

SL6

x86\_64

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

i386

thunderbird-52.3.0-1.el6\_9

thunderbird-debuginfo-52.3.0-1.el6\_9

### 178488 - Gentoo Linux GLSA-201708-09 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7392, CVE-2017-9153

#### Description

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

GLSA-201708-09

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201708-09>

Affected packages:

media-gfx/autotrace <= 0.31.1-r8

### 185855 - Ubuntu Linux 16.04 USN-3404-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7487

#### Description

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

USN-3404-2

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004027.html>

Ubuntu 16.04

linux-image-4.10.0-33-lowlatency\_4.10.0-33.37~16.04.1

linux-image-4.10.0-33-generic-lpae\_4.10.0-33.37~16.04.1

linux-image-4.10.0-33-generic\_4.10.0-33.37~16.04.1

linux-image-lowlatency-hwe-16.04\_4.10.0.33.35

linux-image-generic-hwe-16.04\_4.10.0.33.35

linux-image-generic-lpae-hwe-16.04\_4.10.0.33.35

## 185856 - Ubuntu Linux 14.04 USN-3406-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7914, CVE-2017-7261, CVE-2017-7273, CVE-2017-7487, CVE-2017-7495, CVE-2017-7616

### Description

The scan detected that the host is missing the following update:  
USN-3406-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004030.html>

Ubuntu 14.04

linux-image-powerpc-e500mc\_3.13.0.129.138  
linux-image-3.13.0-129-generic-lpae\_3.13.0-129.178  
linux-image-powerpc-e500\_3.13.0.129.138  
linux-image-3.13.0-129-powerpc64-emb\_3.13.0-129.178  
linux-image-3.13.0-129-powerpc-e500mc\_3.13.0-129.178  
linux-image-powerpc64-smp\_3.13.0.129.138  
linux-image-lowlatency\_3.13.0.129.138  
linux-image-3.13.0-129-powerpc64-smp\_3.13.0-129.178  
linux-image-generic-lpae\_3.13.0.129.138  
linux-image-powerpc-smp\_3.13.0.129.138  
linux-image-3.13.0-129-generic\_3.13.0-129.178  
linux-image-3.13.0-129-powerpc-e500\_3.13.0-129.178  
linux-image-3.13.0-129-powerpc-smp\_3.13.0-129.178  
linux-image-3.13.0-129-lowlatency\_3.13.0-129.178  
linux-image-powerpc64-emb\_3.13.0.129.138  
linux-image-generic\_3.13.0.129.138

## 185858 - Ubuntu Linux 17.04 USN-3404-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7487

### Description

The scan detected that the host is missing the following update:  
USN-3404-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004026.html>

Ubuntu 17.04

linux-image-raspi2\_4.10.0.1016.17  
linux-image-generic\_4.10.0.33.33  
linux-image-4.10.0-33-generic\_4.10.0-33.37

linux-image-4.10.0-1016-raspi2\_4.10.0-1016.19  
linux-image-lowlatency\_4.10.0.33.33  
linux-image-4.10.0-33-lowlatency\_4.10.0-33.37  
linux-image-4.10.0-33-generic-lpae\_4.10.0-33.37  
linux-image-generic-lpae\_4.10.0.33.33

### 185859 - Ubuntu Linux 12.04 USN-3406-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7914, CVE-2017-7261, CVE-2017-7273, CVE-2017-7487, CVE-2017-7495, CVE-2017-7616

#### Description

The scan detected that the host is missing the following update:  
USN-3406-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004031.html>

Ubuntu 12.04

linux-image-3.13.0-129-generic\_3.13.0-129.178~precise1  
linux-image-3.13.0-129-generic-lpae\_3.13.0-129.178~precise1  
linux-image-generic-lts-trusty\_3.13.0.129.119  
linux-image-generic-lpae-lts-trusty\_3.13.0.129.119

### 185861 - Ubuntu Linux 12.04 USN-3199-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7459

#### Description

The scan detected that the host is missing the following update:  
USN-3199-3

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004024.html>

Ubuntu 12.04

python-crypto\_2.4.1-1ubuntu0.2  
python3-crypto\_2.4.1-1ubuntu0.2

### 192572 - Fedora Linux 25 FEDORA-2017-73f71456d7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-12134, CVE-2017-7533

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-73f71456d7

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 25

kernel-4.12.8-200.fc25

## **192573 - Fedora Linux 26 FEDORA-2017-b8fa8e1a13 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-8309, CVE-2017-8379

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-b8fa8e1a13

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

xen-4.8.1-7.fc26

## **192575 - Fedora Linux 26 FEDORA-2017-4336d64e21 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-12134

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-4336d64e21

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

kernel-4.12.8-300.fc26

## 192577 - Fedora Linux 26 FEDORA-2017-8bd521abc9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7555

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-8bd521abc9

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

augeas-1.8.1-1.fc26

## 192578 - Fedora Linux 26 FEDORA-2017-67a3755b96 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12562

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-67a3755b96

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

libsndfile-1.0.28-6.fc26

## 192584 - Fedora Linux 25 FEDORA-2017-9148fe36b9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7546, CVE-2017-7547, CVE-2017-7548

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-9148fe36b9

### Observation

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

Fedora Core 25

postgresql-9.5.8-1.fc25

### 22301 - Solar Controls Heating Control Downloader Uncontrolled Search Path Element Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-9646

#### Description

A vulnerability is present in some versions of Solar Control HCDownloader.

#### Observation

Solar Control is used in electronic systems for renewable energy sources and home automation.

A vulnerability is present in some versions of Solar Control HCDownloader. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

### 130860 - Debian Linux 9.0 DSA-3957-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11399, CVE-2017-11665, CVE-2017-11719, CVE-2017-9608, CVE-2017-9993

#### Description

The scan detected that the host is missing the following update:  
DSA-3957-1

#### Observation

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

<http://www.debian.org/security/2017/dsa-3957>

Debian 9.0

all

ffmpeg\_7:3.2.7-1~deb9u1

### 130863 - Debian Linux 8.0 DSA-3954-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10115, CVE-2017-10116, CVE-2017-10118, CVE-2017-10135, CVE-2017-10176, CVE-2017-10193, CVE-2017-10198, CVE-2017-10243

#### Description

The scan detected that the host is missing the following update:  
DSA-3954-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3954>

Debian 8.0

all

openjdk-7-jre\_7u151-2.6.11-1~deb8u1  
openjdk-7-jre-lib\_7u151-2.6.11-1~deb8u1  
openjdk-7-jre-zero\_7u151-2.6.11-1~deb8u1  
openjdk-7-jdk\_7u151-2.6.11-1~deb8u1  
openjdk-7-dbg\_7u151-2.6.11-1~deb8u1  
openjdk-7-demo\_7u151-2.6.11-1~deb8u1  
icedtea-7-jre-jamvm\_7u151-2.6.11-1~deb8u1  
openjdk-7-jre-headless\_7u151-2.6.11-1~deb8u1  
openjdk-7-source\_7u151-2.6.11-1~deb8u1  
openjdk-7-doc\_7u151-2.6.11-1~deb8u1

### **130865 - Debian Linux 8.0, 9.0 DSA-3958-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11568, CVE-2017-11569, CVE-2017-11571, CVE-2017-11572, CVE-2017-11574, CVE-2017-11575, CVE-2017-11576, CVE-2017-11577

### Description

The scan detected that the host is missing the following update:  
DSA-3958-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3958>

Debian 8.0

all

fontforge\_20120731.b-5+deb8u1

Debian 9.0

all

fontforge\_1:20161005~dfsg-4+deb9u1

### **130866 - Debian Linux 8.0, 9.0 DSA-3952-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

### Description

The scan detected that the host is missing the following update:  
DSA-3952-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3952>

Debian 8.0  
all  
libxml2\_2.9.1+dfsg1-5+deb8u5

Debian 9.0  
all  
libxml2\_2.9.4+dfsg1-2.2+deb9u1

## 141697 - Red Hat Enterprise Linux RHSA-2017-2530 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10087, CVE-2017-10089, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10115, CVE-2017-10116, CVE-2017-10243

### Description

The scan detected that the host is missing the following update:  
RHSA-2017-2530

### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00075.html>

RHEL6D  
x86\_64  
java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

i386  
java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

RHEL6S  
i386  
java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9

java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

x86\_64

java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

RHEL6WS

x86\_64

java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

i386

java-1.6.0-ibm-plugin-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-devel-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-javacomm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-src-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-demo-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-1.6.0.16.50-1jpp.1.el6\_9  
java-1.6.0-ibm-jdbc-1.6.0.16.50-1jpp.1.el6\_9

## 145497 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2263-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10078, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10111, CVE-2017-10115, CVE-2017-10116, CVE-2017-10125, CVE-2017-10243

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2263-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003159.html>

SuSE SLES 12 SP3

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr4.10-30.5.1  
java-1\_8\_0-ibm-1.8.0\_sr4.10-30.5.1  
java-1\_8\_0-ibm-alsa-1.8.0\_sr4.10-30.5.1

SuSE SLES 12 SP2

x86\_64

java-1\_8\_0-ibm-plugin-1.8.0\_sr4.10-30.5.1

java-1\_8\_0-ibm-1.8.0\_sr4.10-30.5.1  
java-1\_8\_0-ibm-alsa-1.8.0\_sr4.10-30.5.1

## 145504 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2280-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10111, CVE-2017-10115, CVE-2017-10116, CVE-2017-10125, CVE-2017-10243

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2280-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003163.html>

SuSE SLES 12 SP3

x86\_64

java-1\_7\_1-ibm-plugin-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-alsa-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-1.7.1\_sr4.10-38.5.1

SuSE SLES 12 SP2

x86\_64

java-1\_7\_1-ibm-plugin-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-alsa-1.7.1\_sr4.10-38.5.1  
java-1\_7\_1-ibm-1.7.1\_sr4.10-38.5.1

## 145505 - SuSE SLES 11 SP4 SUSE-SU-2017:2281-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10053, CVE-2017-10067, CVE-2017-10074, CVE-2017-10081, CVE-2017-10087, CVE-2017-10089, CVE-2017-10090, CVE-2017-10096, CVE-2017-10101, CVE-2017-10102, CVE-2017-10105, CVE-2017-10107, CVE-2017-10108, CVE-2017-10109, CVE-2017-10110, CVE-2017-10111, CVE-2017-10115, CVE-2017-10116, CVE-2017-10125, CVE-2017-10243

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2281-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003164.html>

SuSE SLES 11 SP4

i586

java-1\_7\_1-ibm-1.7.1\_sr4.10-26.5.1

java-1\_7\_1-ibm-alsa-1.7.1\_sr4.10-26.5.1  
java-1\_7\_1-ibm-plugin-1.7.1\_sr4.10-26.5.1  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr4.10-26.5.1

x86\_64

java-1\_7\_1-ibm-1.7.1\_sr4.10-26.5.1  
java-1\_7\_1-ibm-alsa-1.7.1\_sr4.10-26.5.1  
java-1\_7\_1-ibm-plugin-1.7.1\_sr4.10-26.5.1  
java-1\_7\_1-ibm-jdbc-1.7.1\_sr4.10-26.5.1

### 178487 - Gentoo Linux GLSA-201708-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7885, CVE-2017-7975, CVE-2017-7976

#### Description

The scan detected that the host is missing the following update:  
GLSA-201708-10

#### Observation

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

<https://security.gentoo.org/glsa/201708-10>

Affected packages:

media-libs/jbig2dec < 0.13-r4

### 185854 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3403-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11714, CVE-2017-9611, CVE-2017-9612, CVE-2017-9726, CVE-2017-9727, CVE-2017-9739, CVE-2017-9835

#### Description

The scan detected that the host is missing the following update:  
USN-3403-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004025.html>

Ubuntu 16.04

ghostscript\_9.18~dfsg~0-0ubuntu2.7  
libgs9\_9.18~dfsg~0-0ubuntu2.7  
ghostscript-x\_9.18~dfsg~0-0ubuntu2.7  
libgs9-common\_9.18~dfsg~0-0ubuntu2.7

Ubuntu 14.04

libgs9\_9.10~dfsg-0ubuntu10.10  
ghostscript\_9.10~dfsg-0ubuntu10.10

ghostscript-x\_9.10~dfsg-0ubuntu10.10  
libgs9-common\_9.10~dfsg-0ubuntu10.10

Ubuntu 17.04

libgs9\_9.19~dfsg+1-0ubuntu7.6  
ghostscript-x\_9.19~dfsg+1-0ubuntu7.6  
libgs9-common\_9.19~dfsg+1-0ubuntu7.6  
ghostscript\_9.19~dfsg+1-0ubuntu7.6

### 192571 - Fedora Linux 26 FEDORA-2017-8d74f1c135 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12678

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-8d74f1c135

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

taglib-1.11.1-5.fc26

### 22165 - (JSA10800) Juniper Junos Jdncpd Daemon Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-2348

#### Description

A denial of service vulnerability is present in some versions of Juniper Junos OS.

#### Observation

Juniper Junos OS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper Junos OS. The flaw lies in the jdncpd service. Successful exploitation could allow a remote attacker to cause a denial of service condition in the target system.

### 22309 - IBM WebSphere Application Server Admin Console Security Vulnerability (swg22006810)

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

Risk Level: Medium

CVE: CVE-2017-1501

#### Description

A vulnerability is present in some versions of IBM WebSphere Application Server.

### Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

A vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in the Web Services security binding settings. Successful exploitation could allow an unauthenticated user to obtain sensitive information.

### **22322 - (SA-CORE-2017-004) Drupal Core Multiple Vulnerabilities**

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

Risk Level: Medium

CVE: CVE-2017-6923, CVE-2017-6924, CVE-2017-6925

### Description

Multiple vulnerabilities are present in some versions of Drupal.

### Observation

Drupal is a popular open source content management system.

Multiple vulnerabilities are present in some versions of Drupal. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions.

### **22328 - (K70191975) F5 BIG-IP Apache Xerces Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-4463

### Description

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

### Observation

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

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

### **22340 - (K13167034) F5 BIG-IP OpenSSL Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2183

### Description

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

### Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in multiple components. Successful exploitation could allow an attacker to obtain sensitive information.

### **141696 - Red Hat Enterprise Linux RHSA-2017-2538 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-7529

### Description

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

RHSA-2017-2538

### Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00078.html>

### RHEL6\_7S

x86\_64

rh-nginx1 10-nginx-debuginfo-1.10.2-8.el6

rh-nginx1 10-nginx-mod-stream-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-perl-1.10.2-8.el6

rh-nginx1 10-nginx-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-xslt-filter-1.10.2-8.el6

rh-nginx1 10-nginx-mod-mail-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-image-filter-1.10.2-8.el6

### RHEL6S

x86\_64

rh-nginx1 10-nginx-debuginfo-1.10.2-8.el6

rh-nginx1 10-nginx-mod-stream-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-perl-1.10.2-8.el6

rh-nginx1 10-nginx-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-xslt-filter-1.10.2-8.el6

rh-nginx1 10-nginx-mod-mail-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-image-filter-1.10.2-8.el6

### RHEL6WS

x86\_64

rh-nginx1 10-nginx-debuginfo-1.10.2-8.el6

rh-nginx1 10-nginx-mod-stream-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-perl-1.10.2-8.el6

rh-nginx1 10-nginx-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-xslt-filter-1.10.2-8.el6

rh-nginx1 10-nginx-mod-mail-1.10.2-8.el6

rh-nginx1 10-nginx-mod-http-image-filter-1.10.2-8.el6

### RHEL7S

x86\_64

rh-nginx1 10-nginx-mod-mail-1.10.2-8.el7

rh-nginx1 10-nginx-mod-http-image-filter-1.10.2-8.el7

rh-nginx1 10-nginx-debuginfo-1.10.2-8.el7

rh-nginx1 10-nginx-mod-http-perl-1.10.2-8.el7

rh-nginx1 10-nginx-mod-stream-1.10.2-8.el7

rh-nginx1 10-nginx-1.10.2-8.el7

rh-nginx1 10-nginx-mod-http-xslt-filter-1.10.2-8.el7

### RHEL7WS

x86\_64

rh-nginx1 10-nginx-mod-mail-1.10.2-8.el7

rh-nginx1 10-nginx-mod-http-image-filter-1.10.2-8.el7

rh-nginx110-nginx-debuginfo-1.10.2-8.el7  
rh-nginx110-nginx-mod-http-perl-1.10.2-8.el7  
rh-nginx110-nginx-mod-stream-1.10.2-8.el7  
rh-nginx110-nginx-1.10.2-8.el7  
rh-nginx110-nginx-mod-http-xslt-filter-1.10.2-8.el7

### 145502 - SuSE SLES 11 SP4 SUSE-SU-2017:2293-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11185

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2017:2293-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003167.html>

SuSE SLES 11 SP4  
i586  
strongswan-doc-4.4.0-6.36.3.1  
strongswan-4.4.0-6.36.3.1

x86\_64  
strongswan-doc-4.4.0-6.36.3.1  
strongswan-4.4.0-6.36.3.1

### 185857 - Ubuntu Linux 16.04, 17.04 USN-3402-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10149

#### Description

The scan detected that the host is missing the following update:  
USN-3402-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-August/004023.html>

Ubuntu 17.04

python-pysaml2\_3.0.0-3ubuntu1.17.04.1  
python3-pysaml2\_3.0.0-3ubuntu1.17.04.1

Ubuntu 16.04

python3-pysaml2\_3.0.0-3ubuntu1.16.04.1  
python-pysaml2\_3.0.0-3ubuntu1.16.04.1

## 192579 - Fedora Linux 26 FEDORA-2017-aecd25b8a9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7529

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-aecd25b8a9

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

nginx-1.12.1-1.fc26

## 192580 - Fedora Linux 25 FEDORA-2017-c27a947af1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7529

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-c27a947af1

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 25

nginx-1.12.1-1.fc25

## 22313 - (K35263486) F5 BIG-IP Libarchive Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-8688

### Description

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

### Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the vCMP component. Successful exploitation

could allow authenticated local attackers to cause a denial-of-service.

### 130864 - Debian Linux 9.0 DSA-3955-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3636, CVE-2017-3641, CVE-2017-3653

#### Description

The scan detected that the host is missing the following update:  
DSA-3955-1

#### Observation

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

<http://www.debian.org/security/2017/dsa-3955>

Debian 9.0

all  
libmariadbclient-dev\_10.1.26-0+deb9u1  
mariadb-test\_10.1.26-0+deb9u1  
mariadb-server-10.1\_10.1.26-0+deb9u1  
mariadb-server-core-10.1\_10.1.26-0+deb9u1  
libmariadbclient18\_10.1.26-0+deb9u1  
libmariadb-dev\_10.1.26-0+deb9u1  
mariadb-plugin-cracklib-password-check\_10.1.26-0+deb9u1  
mariadb-plugin-oqgraph\_10.1.26-0+deb9u1  
libmariadbclient-dev-compat\_10.1.26-0+deb9u1  
mariadb-plugin-spider\_10.1.26-0+deb9u1  
mariadb-plugin-connect\_10.1.26-0+deb9u1  
mariadb-client\_10.1.26-0+deb9u1  
mariadb-plugin-gssapi-server\_10.1.26-0+deb9u1  
mariadb-test-data\_10.1.26-0+deb9u1  
mariadb-common\_10.1.26-0+deb9u1  
mariadb-plugin-tokudb\_10.1.26-0+deb9u1  
mariadb-plugin-gssapi-client\_10.1.26-0+deb9u1  
mariadb-server\_10.1.26-0+deb9u1  
mariadb-client-core-10.1\_10.1.26-0+deb9u1  
mariadb-client-10.1\_10.1.26-0+deb9u1  
libmariadb18\_10.1.26-0+deb9u1  
mariadb-plugin-mroonga\_10.1.26-0+deb9u1

### 141694 - Red Hat Enterprise Linux RHSA-2017-2533 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2775

#### Description

The scan detected that the host is missing the following update:  
RHSA-2017-2533

#### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-August/msg00076.html>

RHEL7\_2S

noarch

bind-license-9.9.4-29.el7\_2.7

x86\_64

bind-libs-9.9.4-29.el7\_2.7

bind-libs-lite-9.9.4-29.el7\_2.7

bind-devel-9.9.4-29.el7\_2.7

bind-pkcs11-utils-9.9.4-29.el7\_2.7

bind-pkcs11-libs-9.9.4-29.el7\_2.7

bind-debuginfo-9.9.4-29.el7\_2.7

bind-lite-devel-9.9.4-29.el7\_2.7

bind-sdb-9.9.4-29.el7\_2.7

bind-sdb-chroot-9.9.4-29.el7\_2.7

bind-pkcs11-9.9.4-29.el7\_2.7

bind-pkcs11-devel-9.9.4-29.el7\_2.7

bind-chroot-9.9.4-29.el7\_2.7

bind-utils-9.9.4-29.el7\_2.7

bind-9.9.4-29.el7\_2.7

### 145495 - SuSE SLES 11 SP4 SUSE-SU-2017:2290-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3635, CVE-2017-3636, CVE-2017-3641, CVE-2017-3648, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

#### Description

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

SUSE-SU-2017:2290-1

#### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2017-August/003166.html>

SuSE SLES 11 SP4

i586

mysql-client-5.5.57-0.39.3.1

mysql-tools-5.5.57-0.39.3.1

libmysql55client18-5.5.57-0.39.3.1

libmysql55client\_r18-5.5.57-0.39.3.1

mysql-5.5.57-0.39.3.1

x86\_64

libmysql55client18-5.5.57-0.39.3.1

libmysql55client\_r18-32bit-5.5.57-0.39.3.1

mysql-client-5.5.57-0.39.3.1

mysql-tools-5.5.57-0.39.3.1

libmysql55client\_r18-5.5.57-0.39.3.1

libmysql55client18-32bit-5.5.57-0.39.3.1

mysql-5.5.57-0.39.3.1

### 182428 - FreeBSD phpmailer XSS In Code Example And Default Exception Handler (c5d79773-8801-11e7-93f7-d43d7e971a1b)

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

Risk Level: Medium

CVE: CVE-2017-11503

#### Description

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

phpmailer -- XSS in code example and default exception handler (c5d79773-8801-11e7-93f7-d43d7e971a1b)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/c5d79773-8801-11e7-93f7-d43d7e971a1b.html>

Affected packages:

phpmailer < 5.2.24

### **182430 - FreeBSD kanboard Multiple Privilege Escalation Vulnerabilities (7d7e05fb-64da-435a-84fb-4061493b89b9)**

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

Risk Level: Medium

CVE: CVE-2017-12850, CVE-2017-12851

#### Description

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

kanboard -- multiple privilege escalation vulnerabilities (7d7e05fb-64da-435a-84fb-4061493b89b9)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/7d7e05fb-64da-435a-84fb-4061493b89b9.html>

Affected packages:

kanboard < 1.0.46

### **182431 - FreeBSD poppler Multiple Denial Of Service Issues (eca2d861-76f4-42ed-89d2-23a2cb396c87)**

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

Risk Level: Medium

CVE: CVE-2017-9775, CVE-2017-9865

#### Description

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

poppler -- multiple denial of service issues (eca2d861-76f4-42ed-89d2-23a2cb396c87)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/eca2d861-76f4-42ed-89d2-23a2cb396c87.html>

Affected packages:

poppler < 0.56.0

### 130862 - Debian Linux 9.0 DSA-3959-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-0379

#### Description

The scan detected that the host is missing the following update:  
DSA-3959-1

#### Observation

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

<http://www.debian.org/security/2017/dsa-3959>

Debian 9.0

all

libcrypt20\_1.7.6-2+deb9u2

### 130867 - Debian Linux 9.0 DSA-3953-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12440

#### Description

The scan detected that the host is missing the following update:  
DSA-3953-1

#### Observation

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

<http://www.debian.org/security/2017/dsa-3953>

Debian 9.0

all

aodh-evaluator\_3.0.0-4+deb9u1

aodh-api\_3.0.0-4+deb9u1

aodh-doc\_3.0.0-4+deb9u1

aodh-notifier\_3.0.0-4+deb9u1

aodh-listener\_3.0.0-4+deb9u1

python-aodh\_3.0.0-4+deb9u1

aodh-expirer\_3.0.0-4+deb9u1

aodh-common\_3.0.0-4+deb9u1

### 130868 - Debian Linux 8.0, 9.0 DSA-3956-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12865

### Description

The scan detected that the host is missing the following update:  
DSA-3956-1

### Observation

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

<http://www.debian.org/security/2017/dsa-3956>

Debian 8.0  
all  
connman\_1.21-1.2+deb8u1

Debian 9.0  
all  
connman\_1.33-3+deb9u1

## **182429 - FreeBSD rubygems Multiple Vulnerabilities (3f6de636-8cdb-11e7-9c71-f0def1fd7ea2)**

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:  
rubygems -- multiple vulnerabilities (3f6de636-8cdb-11e7-9c71-f0def1fd7ea2)

### Observation

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

<http://www.vuxml.org/freebsd/3f6de636-8cdb-11e7-9c71-f0def1fd7ea2.html>

Affected packages:  
ruby22-gems < 2.6.13  
ruby23-gems < 2.6.13  
ruby24-gems < 2.6.13

## **192569 - Fedora Linux 26 FEDORA-2017-bf74db7147 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-bf74db7147

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

krb5-1.15.1-25.fc26

### 192570 - Fedora Linux 26 FEDORA-2017-f03b04acbb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000115, CVE-2017-1000116

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-f03b04acbb

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

mercurial-4.2.3-1.fc26

### 192574 - Fedora Linux 26 FEDORA-2017-721314e3b3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-721314e3b3

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

java-1.8.0-openjdk-aarch32-1.8.0.141-2.170721.fc26

### 192576 - Fedora Linux 25 FEDORA-2017-97eb475d93 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12836

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-97eb475d93

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 25

cvs-1.11.23-41.fc25

### **192581 - Fedora Linux 26 FEDORA-2017-e5a78c5ca9 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2017-12836

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-e5a78c5ca9

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 26

cvs-1.11.23-42.fc26

### **192582 - Fedora Linux 25 FEDORA-2017-be3df4fe14 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-be3df4fe14

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=1>

Fedora Core 25

java-1.8.0-openjdk-aarch32-1.8.0.141-1.170721.fc25

### **192583 - Fedora Linux 26 FEDORA-2017-0dfa70ae35 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-0dfa70ae35

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/8/?count=200&page=2>

Fedora Core 26

thunderbird-52.3.0-1.fc26

## 22312 - (K90803619) F5 BIG-IP Linux kernel vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-6136

### Description

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

### Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the Linux Kernel. Successful exploitation could allow authenticated local attackers to disclose local information.

## 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.

## 22308 - (CTX225941) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12134, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855

### Update Details

Risk is updated

## 33222 - Oracle Solaris 125720-70 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2006-1526, CVE-2006-3467, CVE-2006-3739, CVE-2006-3740, CVE-2007-5958, CVE-2010-1166, CVE-2011-2895, CVE-2011-4028, CVE-2013-1981, CVE-2013-1982, CVE-2013-1983, CVE-2013-1984, CVE-2013-1985, CVE-2013-1986, CVE-2013-1987, CVE-2013-1988, CVE-2013-1989, CVE-2013-1990, CVE-2013-1992, CVE-2013-1993, CVE-2013-1995, CVE-2013-1996, CVE-2013-1997, CVE-2013-1998, CVE-2013-1999, CVE-2013-2000, CVE-2013-2001, CVE-2013-2002, CVE-2013-2003, CVE-2013-2004, CVE-2013-2005, CVE-2013-2062, CVE-2013-2063, CVE-2013-2064, CVE-2013-2066, CVE-2013-4396, CVE-2014-0209, CVE-2014-0210,

CVE-2014-0211, CVE-2014-0397

Update Details

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

**130840 - Debian Linux 8.0, 9.0 DSA-3932-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-8734, CVE-2017-9800

Update Details

Risk is updated

**130854 - Debian Linux 8.0, 9.0 DSA-3949-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-7555

Update Details

Risk is updated

**182420 - FreeBSD salt Maliciously Crafted Minion IDs Can Cause Unwanted Directory Traversals On The Salt-master (3531141d-a708-477c-954a-**

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

Risk Level: High

CVE: CVE-2017-12791

Update Details

Risk is updated

**184847 - Ubuntu Linux 12.04, 14.04, 14.10, 15.04 USN-2609-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-1324, CVE-2015-1325

Update Details

Risk is updated

**185851 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3400-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2017-7555

Update Details

Risk is updated

### 188837 - Fedora Linux 21 FEDORA-2015-1134 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9637, CVE-2015-1395

[Update Details](#)

Risk is updated

### 189074 - Fedora Linux 20 FEDORA-2015-1165 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9637, CVE-2015-1395

[Update Details](#)

Risk is updated

### 191560 - Fedora Linux 25 FEDORA-2016-2361e1e07a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6812, CVE-2016-8739

[Update Details](#)

Risk is updated

### 192504 - Fedora Linux 26 FEDORA-2017-951b6a78d4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9800

[Update Details](#)

Risk is updated

### 192553 - Fedora Linux 25 FEDORA-2017-1d1a38bdd1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-9800

[Update Details](#)

Risk is updated

### 22282 - (SYM17-006) Symantec Messaging Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-6327, CVE-2017-6328

[Update Details](#)

Risk is updated

**22283 - (SYM17-006) Symantec Messaging Gateway Multiple Vulnerabilities**

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

Risk Level: Medium

CVE: CVE-2017-6327, CVE-2017-6328

[Update Details](#)

Risk is updated

**22287 - Fuji Electric Monitouch V-SFT Multiple Vulnerabilities Prior To 5.4.43.0**

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

Risk Level: Medium

CVE: CVE-2017-9659, CVE-2017-9660, CVE-2017-9662

[Update Details](#)

Risk is updated

**130664 - Debian Linux 8.0 DSA-3756-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-5208

[Update Details](#)

Risk is updated

**145164 - SuSE Linux 13.2 openSUSE-SU-2017:0168-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5331, CVE-2017-5332, CVE-2017-5333

[Update Details](#)

Risk is updated

**181468 - FreeBSD elasticsearch Security Fix For Shared File-system Repositories (23232028-1ba4-11e5-b43d-002590263bf5)**

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

Risk Level: Medium

CVE: CVE-2015-4165

[Update Details](#)

Risk is updated

**182271 - FreeBSD icoutils Check\_offset Overflow On 64-bit Systems (57facd35-ddf6-11e6-915d-001b3856973b)**

---

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5331, CVE-2017-5332, CVE-2017-5333

[Update Details](#)

Risk is updated

#### **182419 - FreeBSD GitLab Two Vulnerabilities (abcc5ad3-7e6a-11e7-93f7-d43d7e971a1b)**

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

Risk Level: Medium

CVE: CVE-2017-12426

[Update Details](#)

Risk is updated

#### **182427 - FreeBSD dnsmdist Multiple Vulnerabilities (198d82f3-8777-11e7-950a-e8e0b747a45a)**

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

Risk Level: Medium

CVE: CVE-2016-7069, CVE-2017-7557

[Update Details](#)

Risk is updated

#### **184929 - Ubuntu Linux 12.04, 14.04, 15.04 USN-2699-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-0839

[Update Details](#)

Risk is updated

#### **185551 - Ubuntu Linux 12.04 USN-3178-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5331, CVE-2017-5332, CVE-2017-5333

[Update Details](#)

Risk is updated

#### **189590 - Fedora Linux 21 FEDORA-2015-11916 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-0839

[Update Details](#)

Risk is updated

#### **189592 - Fedora Linux 22 FEDORA-2015-11723 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-0839

[Update Details](#)

Risk is updated

#### **190326 - Fedora Linux 23 FEDORA-2016-4d0e6ba888 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5258

[Update Details](#)

Risk is updated

#### **191608 - Fedora Linux 24 FEDORA-2017-7c221d6f49 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333

[Update Details](#)

Risk is updated

#### **191612 - Fedora Linux 25 FEDORA-2017-3d7734a8b2 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333

[Update Details](#)

Risk is updated

#### **22288 - Apache Tomcat Multiple Vulnerabilities Prior To 9.0.0.M22**

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

Risk Level: Medium

CVE: CVE-2017-7674, CVE-2017-7675

[Update Details](#)

Risk is updated

#### **22303 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.16**

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

Risk Level: Medium

CVE: CVE-2017-7674, CVE-2017-7675

[Update Details](#)

Risk is updated

#### **91956 - Oracle Enterprise Linux ELSA-2015-2237 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-2675

[Update Details](#)

Risk is updated

#### **130350 - Debian Linux 7.0, 8.0 DSA-3431-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-7944, CVE-2015-7945

[Update Details](#)

Risk is updated

#### **130634 - Debian Linux 8.0 DSA-3720-1 Update Is Not Installed**

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

#### **130636 - Debian Linux 8.0 DSA-3721-1 Update Is Not Installed**

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

#### **130665 - Debian Linux 8.0 DSA-3754-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-8745

[Update Details](#)

Risk is updated

#### **130669 - Debian Linux 8.0 DSA-3755-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-8745

[Update Details](#)

Risk is updated

#### **130835 - Debian Linux 8.0, 9.0 DSA-3924-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-12425

[Update Details](#)

Risk is updated

#### **141007 - Red Hat Enterprise Linux RHSA-2015-2237 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-2675

[Update Details](#)

Risk is updated

#### **141668 - Red Hat Enterprise Linux RHSA-2017-2247 Update Is Not Installed**

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

#### **145474 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2143-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11185

[Update Details](#)

Risk is updated

#### **174873 - Scientific Linux Security ERRATA Low: rest on SL7.x x86\_64 (1512-15662)**

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

Risk Level: Medium

CVE: CVE-2015-2675

[Update Details](#)

Risk is updated

#### **175212 - Scientific Linux Security ERRATA Low: tomcat on SL7.x (noarch) (1708-8410)**

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

#### **182242 - FreeBSD tomcat Multiple Vulnerabilities (3ae106e2-d521-11e6-ae1b-002590263bf5)**

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

#### **182253 - FreeBSD tomcat Information Disclosure Vulnerability (e5ec2767-d529-11e6-ae1b-002590263bf5)**

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

Risk Level: Medium

CVE: CVE-2016-8745

[Update Details](#)

Risk is updated

#### **185842 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3397-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11185

[Update Details](#)

Risk is updated

#### **189073 - Fedora Linux 21 FEDORA-2015-4807 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-1783

[Update Details](#)

Risk is updated

#### **189082 - Fedora Linux 20 FEDORA-2015-4848 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-1783

[Update Details](#)

Risk is updated

#### **189144 - Fedora Linux 22 FEDORA-2015-4821 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-1783

[Update Details](#)

Risk is updated

#### **190645 - Fedora Linux 24 FEDORA-2016-266a26df2b Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-4456

[Update Details](#)

Risk is updated

#### **190923 - Fedora Linux 23 FEDORA-2016-c61cda2beb Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-4456

[Update Details](#)

Risk is updated

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

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

Risk Level: Medium

CVE: CVE-2016-8745

[Update Details](#)

Risk is updated

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

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

Risk Level: Medium

CVE: CVE-2016-8745

[Update Details](#)

Risk is updated

#### **191798 - Fedora Linux 25 FEDORA-2017-d62c8f91e4 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-3156

[Update Details](#)

Risk is updated

#### **192509 - Fedora Linux 25 FEDORA-2017-bfbc5de1b1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-12425

[Update Details](#)

Risk is updated

#### **192515 - Fedora Linux 26 FEDORA-2017-8f4fba5afa Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-12425

[Update Details](#)

Risk is updated

#### **192416 - Fedora Linux 26 FEDORA-2017-e5b36383f4 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11368

[Update Details](#)

Risk is updated

#### **192425 - Fedora Linux 25 FEDORA-2017-8e9d9771c4 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11368

[Update Details](#)

Risk is updated

#### **192432 - Fedora Linux 24 FEDORA-2017-71c47e1e82 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-11368

[Update Details](#)

Risk is updated

## 192554 - Fedora Linux 26 FEDORA-2017-f8f4cd5b67 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12843

### Update Details

Risk is updated

## HOW TO UPDATE

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

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

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

## MCAFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

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

Copyright 2017 McAfee, Inc.

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