

## 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

#### 91969 - Oracle Enterprise Linux ELSA-2015-2152 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2010-5313, CVE-2013-7421, CVE-2014-3601, CVE-2014-3610, CVE-2014-3647, CVE-2014-4014, CVE-2014-7842, CVE-2014-8159, CVE-2014-8171, CVE-2014-8480, CVE-2014-8559, CVE-2014-8989, CVE-2014-9419, CVE-2014-9420, CVE-2014-9529, CVE-2014-9584, CVE-2014-9585, CVE-2014-9644, CVE-2014-9715, CVE-2015-0239, CVE-2015-0275, CVE-2015-1333, CVE-2015-1421, CVE-2015-1573, CVE-2015-1593, CVE-2015-1805, CVE-2015-2666, CVE-2015-2830, CVE-2015-2922, CVE-2015-2925, CVE-2015-3212, CVE-2015-3331, CVE-2015-3339, CVE-2015-3636, CVE-2015-4170, CVE-2015-4700, CVE-2015-5156, CVE-2015-5283, CVE-2015-5364, CVE-2015-5366, CVE-2015-6526, CVE-2015-7613, CVE-2015-7837

#### Description

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

ELSA-2015-2152

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2015-November/005581.html>

OEL7

x86\_64

kernel-devel-3.10.0-327.el7

kernel-3.10.0-327.el7

kernel-tools-3.10.0-327.el7

kernel-debug-devel-3.10.0-327.el7

kernel-headers-3.10.0-327.el7

perf-3.10.0-327.el7

python-perf-3.10.0-327.el7

kernel-abi-whitelists-3.10.0-327.el7

kernel-debug-3.10.0-327.el7

kernel-tools-libs-3.10.0-327.el7

kernel-tools-libs-devel-3.10.0-327.el7

kernel-doc-3.10.0-327.el7

#### 141024 - Red Hat Enterprise Linux RHSA-2015-2518 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4805, CVE-2015-4806, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4883, CVE-2015-4902, CVE-2015-4903

#### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2518

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2518.html>

### RHEL5S

i386

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-accessibility-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el5

x86\_64

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-accessibility-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el5

### RHEL6D

x86\_64

java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7

i386

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7

### RHEL6S

i386

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7

x86\_64

java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7

java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7

#### RHEL6WS

x86\_64  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7

#### i386

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el6\_7  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el6\_7

#### RHEL5D

x86\_64  
java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-accessibility-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el5

#### i386

java-1.5.0-ibm-jdbc-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-javacomm-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-src-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-accessibility-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-plugin-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-demo-1.5.0.16.14-1jpp.1.el5  
java-1.5.0-ibm-devel-1.5.0.16.14-1jpp.1.el5

## 19329 - Red Hat JBoss Apache Commons Remote Code Execution

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

Risk Level: High

CVE: CVE-2015-7501

### Description

A vulnerability in some versions of Red Hat JBoss could lead to remote code execution.

### Observation

A vulnerability in some versions of Red Hat JBoss could lead to remote code execution.

The flaw lies in the Apache Commons Collections library. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 91961 - Oracle Enterprise Linux ELSA-2015-2233 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8240, CVE-2014-8241

### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2233

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005578.html>

OEL7

x86\_64

tigervnc-server-1.3.1-3.el7

tigervnc-server-minimal-1.3.1-3.el7

tigervnc-server-applet-1.3.1-3.el7

tigervnc-server-module-1.3.1-3.el7

tigervnc-license-1.3.1-3.el7

tigervnc-1.3.1-3.el7

tigervnc-icons-1.3.1-3.el7

## 91965 - Oracle Enterprise Linux ELSA-2015-2519 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7189, CVE-2015-7193, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2519

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005588.html>

<http://oss.oracle.com/pipermail/el-errata/2015-November/005589.html>

OEL7

x86\_64

thunderbird-38.4.0-1.0.1.el7\_2

OEL6

x86\_64

thunderbird-38.4.0-1.0.1.el6\_7

i386

thunderbird-38.4.0-1.0.1.el6\_7

## 91966 - Oracle Enterprise Linux ELSA-2015-2522 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

#### Description

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

ELSA-2015-2522

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2015-November/005594.html>

OEL7

x86\_64

apache-commons-collections-3.2.1-22.el7\_2

apache-commons-collections-testframework-javadoc-3.2.1-22.el7\_2

apache-commons-collections-testframework-3.2.1-22.el7\_2

apache-commons-collections-javadoc-3.2.1-22.el7\_2

### **91967 - Oracle Enterprise Linux ELSA-2015-2199 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2013-7423, CVE-2015-1472, CVE-2015-1473, CVE-2015-1781

#### Description

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

ELSA-2015-2199

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2015-November/005577.html>

OEL7

x86\_64

glibc-2.17-105.0.1.el7

glibc-static-2.17-105.0.1.el7

glibc-devel-2.17-105.0.1.el7

glibc-headers-2.17-105.0.1.el7

glibc-utils-2.17-105.0.1.el7

nscd-2.17-105.0.1.el7

glibc-common-2.17-105.0.1.el7

### **91968 - Oracle Enterprise Linux ELSA-2015-2172 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-5277

#### Description

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

ELSA-2015-2172

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005583.html>

### OEL7

x86\_64  
glibc-common-2.17-106.0.1.el7\_2.1  
glibc-utils-2.17-106.0.1.el7\_2.1  
nscd-2.17-106.0.1.el7\_2.1  
glibc-2.17-106.0.1.el7\_2.1  
glibc-headers-2.17-106.0.1.el7\_2.1  
glibc-devel-2.17-106.0.1.el7\_2.1  
glibc-static-2.17-106.0.1.el7\_2.1

## 91970 - Oracle Enterprise Linux ELSA-2015-2521 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2521

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005595.html>

### OEL6

x86\_64  
jakarta-commons-collections-testframework-javadoc-3.2.1-3.5.el6\_7  
jakarta-commons-collections-3.2.1-3.5.el6\_7  
jakarta-commons-collections-testframework-3.2.1-3.5.el6\_7  
jakarta-commons-collections-tomcat5-3.2.1-3.5.el6\_7  
jakarta-commons-collections-javadoc-3.2.1-3.5.el6\_7

### i386

jakarta-commons-collections-testframework-javadoc-3.2.1-3.5.el6\_7  
jakarta-commons-collections-3.2.1-3.5.el6\_7  
jakarta-commons-collections-testframework-3.2.1-3.5.el6\_7  
jakarta-commons-collections-tomcat5-3.2.1-3.5.el6\_7  
jakarta-commons-collections-javadoc-3.2.1-3.5.el6\_7

## 130326 - Debian Linux 7.0, 8.0 DSA-3406-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7183

### Description

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

#### Observation

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

<http://www.debian.org/security/2015/dsa-3406>

Debian 8.0

all

libspr4\_2:4.10.7-1+deb8u1

libspr4-dev\_2:4.10.7-1+deb8u1

libspr4-0d\_2:4.10.7-1+deb8u1

libspr4-dbg\_2:4.10.7-1+deb8u1

Debian 7.0

all

libspr4-dev\_2:4.9.2-1+deb7u3

libspr4\_2:4.9.2-1+deb7u3

libspr4-0d\_2:4.9.2-1+deb7u3

libspr4-dbg\_2:4.9.2-1+deb7u3

### 141019 - Red Hat Enterprise Linux RHSA-2015-2520 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7704

#### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2520

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2520.html>

RHEL6\_5S

i386

ntp-debuginfo-4.2.6p5-2.el6\_5.1

ntp-4.2.6p5-2.el6\_5.1

ntp-perl-4.2.6p5-2.el6\_5.1

ntpdate-4.2.6p5-2.el6\_5.1

noarch

ntp-doc-4.2.6p5-2.el6\_5.1

x86\_64

ntp-debuginfo-4.2.6p5-2.el6\_5.1

ntp-4.2.6p5-2.el6\_5.1

ntp-perl-4.2.6p5-2.el6\_5.1

ntpdate-4.2.6p5-2.el6\_5.1

RHEL6\_6S

i386

ntp-debuginfo-4.2.6p5-3.el6\_6.1  
ntp-4.2.6p5-3.el6\_6.1  
ntpdate-4.2.6p5-3.el6\_6.1

x86\_64  
ntp-debuginfo-4.2.6p5-3.el6\_6.1  
ntp-4.2.6p5-3.el6\_6.1  
ntpdate-4.2.6p5-3.el6\_6.1

## 141020 - Red Hat Enterprise Linux RHSA-2015-2522 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

### Description

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

RHSA-2015-2522

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2015-2522.html>

### RHEL7D

noarch  
apache-commons-collections-3.2.1-22.el7\_2  
apache-commons-collections-testframework-javadoc-3.2.1-22.el7\_2  
apache-commons-collections-testframework-3.2.1-22.el7\_2  
apache-commons-collections-javadoc-3.2.1-22.el7\_2

### RHEL7S

noarch  
apache-commons-collections-3.2.1-22.el7\_2  
apache-commons-collections-testframework-javadoc-3.2.1-22.el7\_2  
apache-commons-collections-testframework-3.2.1-22.el7\_2  
apache-commons-collections-javadoc-3.2.1-22.el7\_2

### RHEL7WS

noarch  
apache-commons-collections-3.2.1-22.el7\_2  
apache-commons-collections-testframework-javadoc-3.2.1-22.el7\_2  
apache-commons-collections-testframework-3.2.1-22.el7\_2  
apache-commons-collections-javadoc-3.2.1-22.el7\_2

## 141021 - Red Hat Enterprise Linux RHSA-2015-2519 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7189, CVE-2015-7193, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

### Description

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

RHSA-2015-2519



## Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2519.html>

### RHEL5S

x86\_64

thunderbird-38.4.0-1.el5\_11

thunderbird-debuginfo-38.4.0-1.el5\_11

i386

thunderbird-38.4.0-1.el5\_11

thunderbird-debuginfo-38.4.0-1.el5\_11

### RHEL6S

i386

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

x86\_64

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

### RHEL6WS

x86\_64

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

i386

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

### RHEL5D

x86\_64

thunderbird-38.4.0-1.el5\_11

thunderbird-debuginfo-38.4.0-1.el5\_11

i386

thunderbird-38.4.0-1.el5\_11

thunderbird-debuginfo-38.4.0-1.el5\_11

### RHEL7D

x86\_64

thunderbird-38.4.0-1.el7\_2

thunderbird-debuginfo-38.4.0-1.el7\_2

### RHEL6D

x86\_64

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

i386

thunderbird-debuginfo-38.4.0-1.el6\_7

thunderbird-38.4.0-1.el6\_7

### RHEL7WS

x86\_64

thunderbird-38.4.0-1.el7\_2

thunderbird-debuginfo-38.4.0-1.el7\_2

## 141022 - Red Hat Enterprise Linux RHSA-2015-2523 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

### Description

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

RHSA-2015-2523

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2015-2523.html>

#### RHEL6\_6S

noarch

rh-java-common-apache-commons-collections-testframework-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-testframework-javadoc-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-javadoc-3.2.1-21.13.el6

#### RHEL6S

noarch

rh-java-common-apache-commons-collections-testframework-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-testframework-javadoc-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-javadoc-3.2.1-21.13.el6

#### RHEL6WS

noarch

rh-java-common-apache-commons-collections-testframework-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-testframework-javadoc-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-3.2.1-21.13.el6

rh-java-common-apache-commons-collections-javadoc-3.2.1-21.13.el6

#### RHEL7S

noarch

rh-java-common-apache-commons-collections-javadoc-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-testframework-javadoc-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-testframework-3.2.1-21.13.el7

#### RHEL7WS

noarch

rh-java-common-apache-commons-collections-javadoc-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-testframework-javadoc-3.2.1-21.13.el7

rh-java-common-apache-commons-collections-testframework-3.2.1-21.13.el7

## 141023 - Red Hat Enterprise Linux RHSA-2015-2521 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7501

### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2521

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2521.html>

#### RHEL6S

noarch  
jakarta-commons-collections-testframework-javadoc-3.2.1-3.5.el6\_7  
jakarta-commons-collections-3.2.1-3.5.el6\_7  
jakarta-commons-collections-testframework-3.2.1-3.5.el6\_7  
jakarta-commons-collections-tomcat5-3.2.1-3.5.el6\_7  
jakarta-commons-collections-javadoc-3.2.1-3.5.el6\_7

#### RHEL6WS

noarch  
jakarta-commons-collections-3.2.1-3.5.el6\_7

#### RHEL6D

noarch  
jakarta-commons-collections-testframework-javadoc-3.2.1-3.5.el6\_7  
jakarta-commons-collections-3.2.1-3.5.el6\_7  
jakarta-commons-collections-testframework-3.2.1-3.5.el6\_7  
jakarta-commons-collections-tomcat5-3.2.1-3.5.el6\_7  
jakarta-commons-collections-javadoc-3.2.1-3.5.el6\_7

## 144069 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2100-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8126

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2100-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00136.html>

#### SuSE Linux 13.1

x86\_64  
libpng16-tools-1.6.6-19.1  
libpng16-devel-32bit-1.6.6-19.1  
libpng16-16-32bit-1.6.6-19.1  
libpng16-16-debuginfo-1.6.6-19.1  
libpng16-compat-devel-1.6.6-19.1  
libpng16-16-debuginfo-32bit-1.6.6-19.1  
libpng16-devel-1.6.6-19.1  
libpng16-debugsource-1.6.6-19.1  
libpng16-16-1.6.6-19.1

libpng16-compat-devel-32bit-1.6.6-19.1  
libpng16-tools-debuginfo-1.6.6-19.1

i586

libpng16-tools-1.6.6-19.1  
libpng16-16-debuginfo-1.6.6-19.1  
libpng16-compat-devel-1.6.6-19.1  
libpng16-devel-1.6.6-19.1  
libpng16-debugsource-1.6.6-19.1  
libpng16-16-1.6.6-19.1  
libpng16-tools-debuginfo-1.6.6-19.1

SuSE Linux 13.2

x86\_64

libpng16-16-32bit-1.6.13-2.7.1  
libpng16-16-debuginfo-1.6.13-2.7.1  
libpng16-16-1.6.13-2.7.1  
libpng16-compat-devel-1.6.13-2.7.1  
libpng16-tools-1.6.13-2.7.1  
libpng16-16-debuginfo-32bit-1.6.13-2.7.1  
libpng16-tools-debuginfo-1.6.13-2.7.1  
libpng16-devel-1.6.13-2.7.1  
libpng16-debugsource-1.6.13-2.7.1  
libpng16-devel-32bit-1.6.13-2.7.1  
libpng16-compat-devel-32bit-1.6.13-2.7.1

i586

libpng16-16-debuginfo-1.6.13-2.7.1  
libpng16-16-1.6.13-2.7.1  
libpng16-compat-devel-1.6.13-2.7.1  
libpng16-tools-1.6.13-2.7.1  
libpng16-tools-debuginfo-1.6.13-2.7.1  
libpng16-devel-1.6.13-2.7.1  
libpng16-debugsource-1.6.13-2.7.1

## 144070 - SuSE Linux 13.2 openSUSE-SU-2015:2130-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8077, CVE-2015-8078

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2130-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00156.html>

SuSE Linux 13.2

x86\_64

perl-Cyrus-IMAP-debuginfo-2.4.18-2.10.1  
cyrus-imapd-snmp-2.4.18-2.10.1  
cyrus-imapd-devel-2.4.18-2.10.1  
perl-Cyrus-IMAP-2.4.18-2.10.1  
cyrus-imapd-snmp-mibs-2.4.18-2.10.1

cyrus-imapd-utils-2.4.18-2.10.1  
perl-Cyrus-SIEVE-managesieve-2.4.18-2.10.1  
perl-Cyrus-SIEVE-managesieve-debuginfo-2.4.18-2.10.1  
cyrus-imapd-2.4.18-2.10.1  
cyrus-imapd-debuginfo-2.4.18-2.10.1  
cyradm-2.4.18-2.10.1  
cyrus-imapd-debugsource-2.4.18-2.10.1

i586

perl-Cyrus-IMAP-debuginfo-2.4.18-2.10.1  
cyrus-imapd-snmp-2.4.18-2.10.1  
cyrus-imapd-devel-2.4.18-2.10.1  
perl-Cyrus-IMAP-2.4.18-2.10.1  
cyrus-imapd-snmp-mibs-2.4.18-2.10.1  
cyrus-imapd-utils-2.4.18-2.10.1  
perl-Cyrus-SIEVE-managesieve-2.4.18-2.10.1  
perl-Cyrus-SIEVE-managesieve-debuginfo-2.4.18-2.10.1  
cyrus-imapd-2.4.18-2.10.1  
cyrus-imapd-debuginfo-2.4.18-2.10.1  
cyradm-2.4.18-2.10.1  
cyrus-imapd-debugsource-2.4.18-2.10.1

## 144074 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2099-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2099-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00135.html>

SuSE Linux 13.1

x86\_64

libpng12-0-debuginfo-32bit-1.2.50-6.7.1  
libpng12-compat-devel-32bit-1.2.50-6.7.1  
libpng12-devel-1.2.50-6.7.1  
libpng12-0-1.2.50-6.7.1  
libpng12-0-32bit-1.2.50-6.7.1  
libpng12-devel-32bit-1.2.50-6.7.1  
libpng12-debugsource-1.2.50-6.7.1  
libpng12-compat-devel-1.2.50-6.7.1  
libpng12-0-debuginfo-1.2.50-6.7.1

i586

libpng12-devel-1.2.50-6.7.1  
libpng12-0-debuginfo-1.2.50-6.7.1  
libpng12-0-1.2.50-6.7.1  
libpng12-compat-devel-1.2.50-6.7.1  
libpng12-debugsource-1.2.50-6.7.1

SuSE Linux 13.2

x86\_64  
libpng12-compat-devel-1.2.51-3.3.1  
libpng12-0-debuginfo-32bit-1.2.51-3.3.1  
libpng12-devel-1.2.51-3.3.1  
libpng12-0-debuginfo-1.2.51-3.3.1  
libpng12-devel-32bit-1.2.51-3.3.1  
libpng12-compat-devel-32bit-1.2.51-3.3.1  
libpng12-0-32bit-1.2.51-3.3.1  
libpng12-0-1.2.51-3.3.1  
libpng12-debugsource-1.2.51-3.3.1

i586  
libpng12-debugsource-1.2.51-3.3.1  
libpng12-compat-devel-1.2.51-3.3.1  
libpng12-0-debuginfo-1.2.51-3.3.1  
libpng12-0-1.2.51-3.3.1  
libpng12-devel-1.2.51-3.3.1

### 160004 - CentOS 5, 6 CESA-2015-2519 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7189, CVE-2015-7193, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

#### Description

The scan detected that the host is missing the following update:  
CESA-2015-2519

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2015-November/021509.html>  
<http://lists.centos.org/pipermail/centos-announce/2015-November/021510.html>

CentOS 5  
x86\_64  
thunderbird-38.4.0-1.el5.centos

i386  
thunderbird-38.4.0-1.el5.centos

CentOS 6  
x86\_64  
thunderbird-38.4.0-1.el6.centos

i686  
thunderbird-38.4.0-1.el6.centos

### 185065 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2819-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4513, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7188, CVE-2015-7189, CVE-2015-7193, CVE-2015-7194, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200

#### Description

The scan detected that the host is missing the following update:  
USN-2819-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003203.html>

Ubuntu 12.04

thunderbird\_38.4.0+build3-0ubuntu0.12.04.1

Ubuntu 15.04

thunderbird\_38.4.0+build3-0ubuntu0.15.04.1

Ubuntu 15.10

thunderbird\_38.4.0+build3-0ubuntu0.15.10.1

Ubuntu 14.04

thunderbird\_38.4.0+build3-0ubuntu0.14.04.1

### **190058 - Fedora Linux 22 FEDORA-2015-a433d8ba72 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-5318, CVE-2015-5320, CVE-2015-5325

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-a433d8ba72

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172686.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172687.html>

Fedora Core 22

jenkins-1.609.3-3.fc22

jenkins-remoting-2.53-1.fc22

### **190059 - Fedora Linux 21 FEDORA-2015-8a1243db75 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8126

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-8a1243db75

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172823.html>

Fedora Core 21

mingw-libpng-1.6.19-1.fc21

### **190067 - Fedora Linux 22 FEDORA-2015-97fc1797fa Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8126

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-97fc1797fa

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172797.html>

Fedora Core 22

mingw-libpng-1.6.19-1.fc22

### **190068 - Fedora Linux 23 FEDORA-2015-13668fff74 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8126

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-13668fff74

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172769.html>

Fedora Core 23

mingw-libpng-1.6.19-1.fc23

### **91962 - Oracle Enterprise Linux ELSA-2015-2355 Update Is Not Installed**

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



Risk Level: Medium  
CVE: CVE-2015-5292

#### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2355

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005579.html>

#### OEL7

x86\_64  
python-sss-murmur-1.13.0-40.el7  
sssd-proxy-1.13.0-40.el7  
sssd-1.13.0-40.el7  
sssd-ipa-1.13.0-40.el7  
python-libsss\_nss\_idmap-1.13.0-40.el7  
sssd-ldap-1.13.0-40.el7  
libsss\_simpleifp-devel-1.13.0-40.el7  
libsss\_simpleifp-1.13.0-40.el7  
sssd-libwbclient-1.13.0-40.el7  
sssd-client-1.13.0-40.el7  
libsss\_nss\_idmap-devel-1.13.0-40.el7  
sssd-krb5-common-1.13.0-40.el7  
python-sss-1.13.0-40.el7  
python-sssdconfig-1.13.0-40.el7  
sssd-common-1.13.0-40.el7  
sssd-common-pac-1.13.0-40.el7  
sssd-libwbclient-devel-1.13.0-40.el7  
libsss\_idmap-1.13.0-40.el7  
libipa\_hbac-1.13.0-40.el7  
sssd-dbus-1.13.0-40.el7  
python-libipa\_hbac-1.13.0-40.el7  
libsss\_nss\_idmap-1.13.0-40.el7  
sssd-krb5-1.13.0-40.el7  
libsss\_idmap-devel-1.13.0-40.el7  
libipa\_hbac-devel-1.13.0-40.el7  
sssd-ad-1.13.0-40.el7  
sssd-tools-1.13.0-40.el7

### **91964 - Oracle Enterprise Linux ELSA-2015-3101 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5283, CVE-2015-7613

#### Description

The scan detected that the host is missing the following update:  
ELSA-2015-3101

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005590.html>  
<http://oss.oracle.com/pipermail/el-errata/2015-November/005591.html>

#### OEL7

x86\_64  
kernel-uek-firmware-3.8.13-118.2.1.el7uek  
kernel-uek-debug-devel-3.8.13-118.2.1.el7uek  
kernel-uek-doc-3.8.13-118.2.1.el7uek  
dtrace-modules-3.8.13-118.2.1.el7uek-0.4.5-3.el7  
kernel-uek-3.8.13-118.2.1.el7uek  
kernel-uek-debug-3.8.13-118.2.1.el7uek  
kernel-uek-devel-3.8.13-118.2.1.el7uek

#### OEL6

x86\_64  
kernel-uek-firmware-3.8.13-118.2.1.el6uek  
kernel-uek-debug-devel-3.8.13-118.2.1.el6uek  
kernel-uek-doc-3.8.13-118.2.1.el6uek  
dtrace-modules-3.8.13-118.2.1.el6uek-0.4.5-3.el6  
kernel-uek-debug-3.8.13-118.2.1.el6uek  
kernel-uek-3.8.13-118.2.1.el6uek  
kernel-uek-devel-3.8.13-118.2.1.el6uek

### 132200 - Oracle VM OVMSA-2015-0150 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5283, CVE-2015-7613

#### Description

The scan detected that the host is missing the following update:  
OVMSA-2015-0150

#### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2015-December/000398.html>

OVM3.3  
x86\_64  
kernel-uek-3.8.13-118.2.1.el6uek  
kernel-uek-firmware-3.8.13-118.2.1.el6uek

### 190048 - Fedora Linux 23 FEDORA-2015-c24af963a2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035, CVE-2015-8242

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-c24af963a2

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172710.html>

Fedora Core 23

libxml2-2.9.3-1.fc23

### **190056 - Fedora Linux 22 FEDORA-2015-037f844d3e Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035, CVE-2015-8242

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-037f844d3e

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172943.html>

Fedora Core 22

libxml2-2.9.3-1.fc22

### **19308 - IBM WebSphere Application Server Java Multiple Vulnerabilities (October 2015 CPU)**

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

Risk Level: Medium

CVE: CVE-2015-4734, CVE-2015-4872, CVE-2015-5006

#### Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

#### Observation

IBM WebSphere Application Server is a Java web application server.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in IBM Java SDK shipped with IBM WebSphere Application Server. Successful exploitation could allow an attacker to obtain sensitive information or affect partial integrity.

### **91960 - Oracle Enterprise Linux ELSA-2015-2505 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5273, CVE-2015-5287, CVE-2015-5302

#### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2505

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005584.html>

### OEL7

x86\_64

libreport-cli-2.1.11-31.0.1.el7  
libreport-rhel-anaconda-bugzilla-2.1.11-31.0.1.el7  
abrt-cli-2.1.11-35.0.1.el7  
abrt-gui-2.1.11-35.0.1.el7  
libreport-gtk-devel-2.1.11-31.0.1.el7  
abrt-gui-devel-2.1.11-35.0.1.el7  
abrt-tui-2.1.11-35.0.1.el7  
abrt-python-doc-2.1.11-35.0.1.el7  
libreport-web-devel-2.1.11-31.0.1.el7  
abrt-addon-vmcore-2.1.11-35.0.1.el7  
libreport-plugin-bugzilla-2.1.11-31.0.1.el7  
abrt-retrace-client-2.1.11-35.0.1.el7  
libreport-devel-2.1.11-31.0.1.el7  
libreport-plugin-ureport-2.1.11-31.0.1.el7  
abrt-python-2.1.11-35.0.1.el7  
libreport-plugin-mailx-2.1.11-31.0.1.el7  
abrt-libs-2.1.11-35.0.1.el7  
abrt-console-notification-2.1.11-35.0.1.el7  
abrt-devel-2.1.11-35.0.1.el7  
libreport-compat-2.1.11-31.0.1.el7  
libreport-2.1.11-31.0.1.el7  
libreport-plugin-logger-2.1.11-31.0.1.el7  
abrt-2.1.11-35.0.1.el7  
abrt-gui-libs-2.1.11-35.0.1.el7  
abrt-addon-kerneloops-2.1.11-35.0.1.el7  
abrt-addon-python-2.1.11-35.0.1.el7  
abrt-addon-ccpp-2.1.11-35.0.1.el7  
abrt-addon-xorg-2.1.11-35.0.1.el7  
libreport-newt-2.1.11-31.0.1.el7  
abrt-addon-pstoreoops-2.1.11-35.0.1.el7  
abrt-addon-upload-watch-2.1.11-35.0.1.el7  
libreport-plugin-reportuploader-2.1.11-31.0.1.el7  
libreport-anaconda-2.1.11-31.0.1.el7  
libreport-python-2.1.11-31.0.1.el7  
libreport-web-2.1.11-31.0.1.el7  
libreport-filesystem-2.1.11-31.0.1.el7  
libreport-gtk-2.1.11-31.0.1.el7  
abrt-desktop-2.1.11-35.0.1.el7  
abrt-dbus-2.1.11-35.0.1.el7  
libreport-rhel-bugzilla-2.1.11-31.0.1.el7  
libreport-plugin-kerneloops-2.1.11-31.0.1.el7

### **91963 - Oracle Enterprise Linux ELSA-2015-2315 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-0272, CVE-2015-2924

### Description

The scan detected that the host is missing the following update:  
ELSA-2015-2315

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2015-November/005580.html>

### OEL7

x86\_64

NetworkManager-libreswan-gnome-1.0.6-3.el7  
NetworkManager-1.0.6-27.0.1.el7  
NetworkManager-wifi-1.0.6-27.0.1.el7  
NetworkManager-adsl-1.0.6-27.0.1.el7  
NetworkManager-bluetooth-1.0.6-27.0.1.el7  
ModemManager-vala-1.1.0-8.git20130913.el7  
NetworkManager-team-1.0.6-27.0.1.el7  
NetworkManager-libreswan-1.0.6-3.el7  
ModemManager-devel-1.1.0-8.git20130913.el7  
NetworkManager-config-routing-rules-1.0.6-27.0.1.el7  
network-manager-applet-1.0.6-2.el7  
ModemManager-glib-1.1.0-8.git20130913.el7  
ModemManager-glib-devel-1.1.0-8.git20130913.el7  
NetworkManager-devel-1.0.6-27.0.1.el7  
nm-connection-editor-1.0.6-2.el7  
libnm-gtk-devel-1.0.6-2.el7  
libnm-gtk-1.0.6-2.el7  
NetworkManager-wwan-1.0.6-27.0.1.el7  
NetworkManager-libnm-devel-1.0.6-27.0.1.el7  
NetworkManager-libnm-1.0.6-27.0.1.el7  
NetworkManager-config-server-1.0.6-27.0.1.el7  
NetworkManager-tui-1.0.6-27.0.1.el7  
ModemManager-1.1.0-8.git20130913.el7  
NetworkManager-glib-devel-1.0.6-27.0.1.el7  
NetworkManager-glib-1.0.6-27.0.1.el7

## **141026 - Red Hat Enterprise Linux RHSA-2015-2515 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2515

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2515.html>

### RHEL7S

x86\_64

git19-git-1.9.4-3.el7.1

git19-git-svn-1.9.4-3.el7.1  
git19-git-debuginfo-1.9.4-3.el7.1  
git19-git-daemon-1.9.4-3.el7.1

noarch

git19-git-hg-1.9.4-3.el7.1  
git19-emacs-git-1.9.4-3.el7.1  
git19-perl-Git-1.9.4-3.el7.1  
git19-emacs-git-el-1.9.4-3.el7.1  
git19-git-email-1.9.4-3.el7.1  
git19-perl-Git-SVN-1.9.4-3.el7.1  
git19-gitk-1.9.4-3.el7.1  
git19-gitweb-1.9.4-3.el7.1  
git19-git-cvs-1.9.4-3.el7.1  
git19-git-bzr-1.9.4-3.el7.1  
git19-git-gui-1.9.4-3.el7.1  
git19-git-all-1.9.4-3.el7.1

RHEL6S

x86\_64

git19-git-daemon-1.9.4-3.el6.1  
git19-git-debuginfo-1.9.4-3.el6.1  
git19-git-1.9.4-3.el6.1  
git19-git-svn-1.9.4-3.el6.1

noarch

git19-git-email-1.9.4-3.el6.1  
git19-git-all-1.9.4-3.el6.1  
git19-perl-Git-1.9.4-3.el6.1  
git19-gitweb-1.9.4-3.el6.1  
git19-perl-Git-SVN-1.9.4-3.el6.1  
git19-emacs-git-1.9.4-3.el6.1  
git19-emacs-git-el-1.9.4-3.el6.1  
git19-git-cvs-1.9.4-3.el6.1  
git19-gitk-1.9.4-3.el6.1  
git19-git-gui-1.9.4-3.el6.1

RHEL6WS

x86\_64

git19-git-daemon-1.9.4-3.el6.1  
git19-git-debuginfo-1.9.4-3.el6.1  
git19-git-1.9.4-3.el6.1  
git19-git-svn-1.9.4-3.el6.1

noarch

git19-git-email-1.9.4-3.el6.1  
git19-git-all-1.9.4-3.el6.1  
git19-perl-Git-1.9.4-3.el6.1  
git19-gitweb-1.9.4-3.el6.1  
git19-perl-Git-SVN-1.9.4-3.el6.1  
git19-emacs-git-1.9.4-3.el6.1  
git19-emacs-git-el-1.9.4-3.el6.1  
git19-git-cvs-1.9.4-3.el6.1  
git19-gitk-1.9.4-3.el6.1  
git19-git-gui-1.9.4-3.el6.1

RHEL6\_6S

x86\_64

git19-git-daemon-1.9.4-3.el6.1  
git19-git-debuginfo-1.9.4-3.el6.1

git19-git-1.9.4-3.el6.1  
git19-git-svn-1.9.4-3.el6.1

noarch  
git19-git-email-1.9.4-3.el6.1  
git19-git-all-1.9.4-3.el6.1  
git19-perl-Git-1.9.4-3.el6.1  
git19-gitweb-1.9.4-3.el6.1  
git19-perl-Git-SVN-1.9.4-3.el6.1  
git19-emacs-git-1.9.4-3.el6.1  
git19-emacs-git-el-1.9.4-3.el6.1  
git19-git-cvs-1.9.4-3.el6.1  
git19-gitk-1.9.4-3.el6.1  
git19-git-gui-1.9.4-3.el6.1

RHEL6\_5S  
x86\_64  
git19-git-daemon-1.9.4-3.el6.1  
git19-git-debuginfo-1.9.4-3.el6.1  
git19-git-1.9.4-3.el6.1  
git19-git-svn-1.9.4-3.el6.1

noarch  
git19-git-email-1.9.4-3.el6.1  
git19-git-all-1.9.4-3.el6.1  
git19-perl-Git-1.9.4-3.el6.1  
git19-gitweb-1.9.4-3.el6.1  
git19-perl-Git-SVN-1.9.4-3.el6.1  
git19-emacs-git-1.9.4-3.el6.1  
git19-emacs-git-el-1.9.4-3.el6.1  
git19-git-cvs-1.9.4-3.el6.1  
git19-gitk-1.9.4-3.el6.1  
git19-git-gui-1.9.4-3.el6.1

RHEL7WS  
x86\_64  
git19-git-1.9.4-3.el7.1  
git19-git-svn-1.9.4-3.el7.1  
git19-git-debuginfo-1.9.4-3.el7.1  
git19-git-daemon-1.9.4-3.el7.1

noarch  
git19-git-hg-1.9.4-3.el7.1  
git19-emacs-git-1.9.4-3.el7.1  
git19-perl-Git-1.9.4-3.el7.1  
git19-emacs-git-el-1.9.4-3.el7.1  
git19-git-email-1.9.4-3.el7.1  
git19-perl-Git-SVN-1.9.4-3.el7.1  
git19-gitk-1.9.4-3.el7.1  
git19-gitweb-1.9.4-3.el7.1  
git19-git-cvs-1.9.4-3.el7.1  
git19-git-bzr-1.9.4-3.el7.1  
git19-git-gui-1.9.4-3.el7.1  
git19-git-all-1.9.4-3.el7.1

#### 144072 - SuSE Linux 13.1 openSUSE-SU-2015:2154-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4813, CVE-2015-4896

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2154-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00172.html>

SuSE Linux 13.1

i586  
virtualbox-guest-kmp-default-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-qt-4.2.36-2.52.2  
virtualbox-host-kmp-pae-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-kmp-desktop-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-4.2.36-2.52.2  
virtualbox-qt-debuginfo-4.2.36-2.52.2  
virtualbox-host-kmp-default-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-host-kmp-default-4.2.36\_k3.11.10\_29-2.52.2  
python-virtualbox-4.2.36-2.52.2  
virtualbox-devel-4.2.36-2.52.2  
virtualbox-debuginfo-4.2.36-2.52.2  
virtualbox-guest-x11-debuginfo-4.2.36-2.52.2  
virtualbox-debugsource-4.2.36-2.52.2  
virtualbox-host-kmp-pae-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-host-kmp-desktop-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-kmp-default-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-kmp-pae-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-x11-4.2.36-2.52.2  
python-virtualbox-debuginfo-4.2.36-2.52.2  
virtualbox-guest-tools-4.2.36-2.52.2  
virtualbox-guest-kmp-desktop-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-websrv-debuginfo-4.2.36-2.52.2  
virtualbox-guest-kmp-pae-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-tools-debuginfo-4.2.36-2.52.2  
virtualbox-host-kmp-desktop-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-websrv-4.2.36-2.52.2

noarch

virtualbox-host-source-4.2.36-2.52.2

x86\_64

virtualbox-guest-kmp-default-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-qt-4.2.36-2.52.2  
virtualbox-guest-kmp-desktop-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-4.2.36-2.52.2  
virtualbox-qt-debuginfo-4.2.36-2.52.2  
virtualbox-host-kmp-default-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-host-kmp-default-4.2.36\_k3.11.10\_29-2.52.2  
python-virtualbox-4.2.36-2.52.2  
virtualbox-devel-4.2.36-2.52.2  
virtualbox-debuginfo-4.2.36-2.52.2  
virtualbox-guest-x11-debuginfo-4.2.36-2.52.2  
virtualbox-debugsource-4.2.36-2.52.2  
virtualbox-host-kmp-desktop-debuginfo-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-guest-kmp-default-4.2.36\_k3.11.10\_29-2.52.2



virtualbox-guest-x11-4.2.36-2.52.2  
python-virtualbox-debuginfo-4.2.36-2.52.2  
virtualbox-guest-tools-4.2.36-2.52.2  
virtualbox-guest-kmp-desktop-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-websrv-debuginfo-4.2.36-2.52.2  
virtualbox-guest-tools-debuginfo-4.2.36-2.52.2  
virtualbox-host-kmp-desktop-4.2.36\_k3.11.10\_29-2.52.2  
virtualbox-websrv-4.2.36-2.52.2

#### 144073 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2116-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5185

##### Description

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

SUSE-SU-2015:2116-1

##### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2015-November/001702.html>

SuSE SLED 12

x86\_64

sblim-sfcb-1.4.8-5.3.3

sblim-sfcb-debugsource-1.4.8-5.3.3

sblim-sfcb-debuginfo-1.4.8-5.3.3

SuSE SLES 12

x86\_64

sblim-sfcb-1.4.8-5.3.3

sblim-sfcb-debugsource-1.4.8-5.3.3

sblim-sfcb-debuginfo-1.4.8-5.3.3

#### 144075 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2103-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8023

##### Description

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

openSUSE-SU-2015:2103-1

##### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00139.html>

SuSE Linux 13.1

i586

strongswan-ipsec-debuginfo-5.1.1-14.1

strongswan-nm-5.1.1-14.1  
strongswan-sqlite-debuginfo-5.1.1-14.1  
strongswan-nm-debuginfo-5.1.1-14.1  
strongswan-libs0-5.1.1-14.1  
strongswan-mysql-5.1.1-14.1  
strongswan-ipsec-5.1.1-14.1  
strongswan-mysql-debuginfo-5.1.1-14.1  
strongswan-debugsource-5.1.1-14.1  
strongswan-libs0-debuginfo-5.1.1-14.1  
strongswan-5.1.1-14.1  
strongswan-sqlite-5.1.1-14.1

noarch  
strongswan-doc-5.1.1-14.1

x86\_64  
strongswan-ipsec-debuginfo-5.1.1-14.1  
strongswan-nm-5.1.1-14.1  
strongswan-sqlite-debuginfo-5.1.1-14.1  
strongswan-nm-debuginfo-5.1.1-14.1  
strongswan-libs0-5.1.1-14.1  
strongswan-mysql-5.1.1-14.1  
strongswan-ipsec-5.1.1-14.1  
strongswan-mysql-debuginfo-5.1.1-14.1  
strongswan-debugsource-5.1.1-14.1  
strongswan-libs0-debuginfo-5.1.1-14.1  
strongswan-5.1.1-14.1  
strongswan-sqlite-5.1.1-14.1

SuSE Linux 13.2

i586  
strongswan-sqlite-5.1.3-4.14.1  
strongswan-nm-5.1.3-4.14.1  
strongswan-mysql-debuginfo-5.1.3-4.14.1  
strongswan-ipsec-5.1.3-4.14.1  
strongswan-sqlite-debuginfo-5.1.3-4.14.1  
strongswan-mysql-5.1.3-4.14.1  
strongswan-5.1.3-4.14.1  
strongswan-ipsec-debuginfo-5.1.3-4.14.1  
strongswan-libs0-5.1.3-4.14.1  
strongswan-libs0-debuginfo-5.1.3-4.14.1  
strongswan-debugsource-5.1.3-4.14.1  
strongswan-nm-debuginfo-5.1.3-4.14.1

noarch  
strongswan-doc-5.1.3-4.14.1

x86\_64  
strongswan-sqlite-5.1.3-4.14.1  
strongswan-nm-5.1.3-4.14.1  
strongswan-mysql-debuginfo-5.1.3-4.14.1  
strongswan-ipsec-5.1.3-4.14.1  
strongswan-sqlite-debuginfo-5.1.3-4.14.1  
strongswan-mysql-5.1.3-4.14.1  
strongswan-5.1.3-4.14.1  
strongswan-ipsec-debuginfo-5.1.3-4.14.1  
strongswan-libs0-5.1.3-4.14.1  
strongswan-libs0-debuginfo-5.1.3-4.14.1  
strongswan-debugsource-5.1.3-4.14.1  
strongswan-nm-debuginfo-5.1.3-4.14.1

## 185069 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2818-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4871

### Description

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

USN-2818-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003200.html>

Ubuntu 15.04

openjdk-7-jre\_7u91-2.6.3-0ubuntu0.15.04.1  
icedtea-7-jre-jamvm\_7u91-2.6.3-0ubuntu0.15.04.1  
openjdk-7-jre-zero\_7u91-2.6.3-0ubuntu0.15.04.1  
openjdk-7-jre-lib\_7u91-2.6.3-0ubuntu0.15.04.1  
openjdk-7-jre-headless\_7u91-2.6.3-0ubuntu0.15.04.1

Ubuntu 15.10

openjdk-7-jre-headless\_7u91-2.6.3-0ubuntu0.15.10.1  
openjdk-7-jre-lib\_7u91-2.6.3-0ubuntu0.15.10.1  
icedtea-7-jre-jamvm\_7u91-2.6.3-0ubuntu0.15.10.1  
openjdk-7-jre\_7u91-2.6.3-0ubuntu0.15.10.1  
openjdk-7-jre-zero\_7u91-2.6.3-0ubuntu0.15.10.1

Ubuntu 14.04

openjdk-7-jre-zero\_7u91-2.6.3-0ubuntu0.14.04.1  
openjdk-7-jre-lib\_7u91-2.6.3-0ubuntu0.14.04.1  
openjdk-7-jre-headless\_7u91-2.6.3-0ubuntu0.14.04.1  
openjdk-7-jre\_7u91-2.6.3-0ubuntu0.14.04.1  
icedtea-7-jre-jamvm\_7u91-2.6.3-0ubuntu0.14.04.1

## 190053 - Fedora Linux 21 FEDORA-2015-1932919218 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4279

### Description

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

FEDORA-2015-1932919218

### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172990.html>

Fedora Core 21

imapsync-1.644-2.fc21

### 190054 - Fedora Linux 22 FEDORA-2015-6691fc09b2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4279

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-6691fc09b2

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172961.html>

Fedora Core 22

imapsync-1.644-2.fc22

### 190066 - Fedora Linux 23 FEDORA-2015-5d1f935811 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4279

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-5d1f935811

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172915.html>

Fedora Core 23

imapsync-1.644-2.fc23

### 144068 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2121-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3310

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2121-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00147.html>

SuSE Linux 13.1

x86\_64

ppp-2.4.7-20.7.1

ppp-debuginfo-2.4.7-20.7.1

ppp-debugsource-2.4.7-20.7.1

ppp-devel-2.4.7-20.7.1

i586

ppp-2.4.7-20.7.1

ppp-debuginfo-2.4.7-20.7.1

ppp-debugsource-2.4.7-20.7.1

ppp-devel-2.4.7-20.7.1

SuSE Linux 13.2

x86\_64

ppp-debuginfo-2.4.7-2.3.1

ppp-debugsource-2.4.7-2.3.1

ppp-devel-2.4.7-2.3.1

ppp-2.4.7-2.3.1

i586

ppp-debuginfo-2.4.7-2.3.1

ppp-debugsource-2.4.7-2.3.1

ppp-devel-2.4.7-2.3.1

ppp-2.4.7-2.3.1

### **185066 - Ubuntu Linux 14.04 USN-2823-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5283, CVE-2015-7872

### Description

The scan detected that the host is missing the following update:  
USN-2823-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003204.html>

Ubuntu 14.04

linux-image-3.13.0-71-lowlatency\_3.13.0-71.114

linux-image-3.13.0-71-powerpc-e500mc\_3.13.0-71.114

linux-image-3.13.0-71-powerpc64-smp\_3.13.0-71.114

linux-image-3.13.0-71-powerpc-e500\_3.13.0-71.114

linux-image-3.13.0-71-powerpc64-emb\_3.13.0-71.114

linux-image-3.13.0-71-generic-lpae\_3.13.0-71.114

linux-image-3.13.0-71-powerpc-smp\_3.13.0-71.114

linux-image-3.13.0-71-generic\_3.13.0-71.114

### 88721 - Slackware Linux 14.1 SSA:2015-328-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3210

#### Description

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

SSA:2015-328-01

#### 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=2015&m=slackware-security.339015>

Slackware 14.1

x86\_64

pcre-8.38-x86\_64-1

### 130321 - Debian Linux 7.0, 8.0 DSA-3405-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-0859

#### Description

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

DSA-3405-1

#### Observation

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

For more information see:

<http://www.debian.org/security/2015/dsa-3405>

Debian 8.0

all

smokeping\_2.6.9-1+deb8u1

Debian 7.0

all

smokeping\_2.6.8-2+deb7u1

### 130322 - Debian Linux 7.0 DSA-3408-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8313

#### Description

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

DSA-3408-1

### Observation

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

<http://www.debian.org/security/2015/dsa-3408>

Debian 7.0

all

libgnutls-openssl27\_2.12.20-8+deb7u4

guile-gnutls\_2.12.20-8+deb7u4

gnutls26-doc\_2.12.20-8+deb7u4

libgnutlsxx27\_2.12.20-8+deb7u4

libgnutls-dev\_2.12.20-8+deb7u4

libgnutls26\_2.12.20-8+deb7u4

libgnutls26-dbg\_2.12.20-8+deb7u4

gnutls-bin\_2.12.20-8+deb7u4

### **130323 - Debian Linux 7.0, 8.0 DSA-3404-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-8213

### Description

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

### Observation

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

<http://www.debian.org/security/2015/dsa-3404>

Debian 8.0

all

python-django\_1.7.7-1+deb8u3

Debian 7.0

all

python-django\_1.4.5-1+deb7u14

### **130324 - Debian Linux 7.0, 8.0 DSA-3407-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-0860

### Description

The scan detected that the host is missing the following update:  
DSA-3407-1

### Observation

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

<http://www.debian.org/security/2015/dsa-3407>

Debian 8.0  
all  
dpkg\_1.17.26

Debian 7.0  
all  
dpkg\_1.16.17

### 130325 - Debian Linux 7.0, 8.0 DSA-3403-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

#### Observation

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

<http://www.debian.org/security/2015/dsa-3403>

Debian 8.0  
all  
libcommons-collections3-java\_3.2.1-7+deb8u1

Debian 7.0  
all  
libcommons-collections3-java\_3.2.1-5+deb7u1

### 130327 - Debian Linux 7.0, 8.0 DSA-3409-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5309

#### Description

The scan detected that the host is missing the following update:  
DSA-3409-1

#### Observation

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

<http://www.debian.org/security/2015/dsa-3409>

Debian 8.0  
all  
putty\_0.63-10+deb8u1

Debian 7.0  
all



## 141025 - Red Hat Enterprise Linux RHSA-2015-2525 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2525

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2525.html>

RHEL6\_5S

i386

redhat-release-server-6Server-6.5.0.3.el6\_5.2

x86\_64

redhat-release-server-6Server-6.5.0.3.el6\_5.2

## 144071 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2153-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-1606, CVE-2015-1607

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2153-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-11/msg00171.html>

SuSE Linux 13.1

i586

gpg2-debugsource-2.0.22-12.1

gpg2-debuginfo-2.0.22-12.1

gpg2-2.0.22-12.1

noarch

gpg2-lang-2.0.22-12.1

x86\_64

gpg2-debugsource-2.0.22-12.1

gpg2-debuginfo-2.0.22-12.1

gpg2-2.0.22-12.1

SuSE Linux 13.2

i586  
gpg2-debugsource-2.0.26-2.3.1  
gpg2-debuginfo-2.0.26-2.3.1  
gpg2-2.0.26-2.3.1

noarch  
gpg2-lang-2.0.26-2.3.1

x86\_64  
gpg2-debugsource-2.0.26-2.3.1  
gpg2-debuginfo-2.0.26-2.3.1  
gpg2-2.0.26-2.3.1

### 181688 - FreeBSD django Information Leak Vulnerability (11c52bc6-97aa-11e5-b8df-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8213

#### Description

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

django -- information leak vulnerability (11c52bc6-97aa-11e5-b8df-14dae9d210b8)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/11c52bc6-97aa-11e5-b8df-14dae9d210b8.html>

Affected packages:

py27-django < 1.8.7  
py32-django < 1.8.7  
py33-django < 1.8.7  
py34-django < 1.8.7  
py27-django17 < 1.7.11  
py32-django17 < 1.7.11  
py33-django17 < 1.7.11  
py34-django17 < 1.7.11  
py27-django-devel <= 20150709,1  
py32-django-devel <= 20150709,1  
py33-django-devel <= 20150709,1  
py34-django-devel <= 20150709,1

### 181689 - FreeBSD cyrus-imapd Integer Overflow In The start\_octet Addition (d62ec98e-97d8-11e5-8c0e-080027b00c2e)

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

Risk Level: Low

CVE: CVE-2015-8077, CVE-2015-8078

#### Description

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

cyrus-imapd -- integer overflow in the start\_octet addition (d62ec98e-97d8-11e5-8c0e-080027b00c2e)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/d62ec98e-97d8-11e5-8c0e-080027b00c2e.html>

Affected packages:

2.5.0 <= cyrus-imapd25 < 2.5.7

2.4.0 <= cyrus-imapd24 < 2.4.18\_2

### **185064 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2820-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-0860

#### Description

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

USN-2820-1

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003201.html>

Ubuntu 12.04

dpkg\_1.16.1.2ubuntu7.7

Ubuntu 15.04

dpkg\_1.17.25ubuntu1.1

Ubuntu 15.10

dpkg\_1.18.2ubuntu5.1

Ubuntu 14.04

dpkg\_1.17.5ubuntu5.5

### **185068 - Ubuntu Linux 12.04, 14.04 USN-2821-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

USN-2821-1

#### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-November/003202.html>

Ubuntu 12.04

libgnutls26\_2.12.14-5ubuntu3.10

Ubuntu 14.04

libgnutls26\_2.12.23-12ubuntu2.3

#### **190045 - Fedora Linux 23 FEDORA-2015-994f0b3021 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-2015-994f0b3021

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172704.html>

Fedora Core 23

pcre-8.38-1.fc23

#### **190046 - Fedora Linux 23 FEDORA-2015-10f92d4d06 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-2015-10f92d4d06

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172884.html>

Fedora Core 23

wget-1.17-1.fc23

#### **190047 - Fedora Linux 22 FEDORA-2015-0de8163795 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-2015-0de8163795

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172804.html>

Fedora Core 22

python-pycurl-7.19.5.1-3.fc22

### **190049 - Fedora Linux 21 FEDORA-2015-6542ab6d3a Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5302

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-6542ab6d3a

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172695.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172694.html>

Fedora Core 21

libreport-2.3.0-10.fc21

abrt-2.3.0-12.fc21

### **190051 - Fedora Linux 22 FEDORA-2015-6fb2c59536 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-2015-6fb2c59536

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172938.html>

Fedora Core 22

ca-certificates-2015.2.6-1.0.fc22

### 190055 - Fedora Linux 21 FEDORA-2015-8f34820159 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-2015-8f34820159

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172805.html>

Fedora Core 21

seamonkey-2.39-1.fc21

### 190057 - Fedora Linux 22 FEDORA-2015-0772f3f93b 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-2015-0772f3f93b

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172944.html>

Fedora Core 22

rpm-4.12.0.1-14.fc22

### 190060 - Fedora Linux 23 FEDORA-2015-f9e5ca4e6a 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-2015-f9e5ca4e6a

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172670.html>

Fedora Core 23

ca-certificates-2015.2.6-1.0.fc23

#### **190061 - Fedora Linux 22 FEDORA-2015-5ad4a1f151 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5309

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-5ad4a1f151

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173094.html>

Fedora Core 22

putty-0.66-1.fc22

#### **190062 - Fedora Linux 23 FEDORA-2015-79c1758468 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5273, CVE-2015-5287

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-79c1758468

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172809.html>

Fedora Core 23

abrt-2.7.1-1.fc23

#### **190064 - Fedora Linux 23 FEDORA-2015-3d17682c15 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5309

##### Description

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

FEDORA-2015-3d17682c15

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/173021.html>

Fedora Core 23

putty-0.66-1.fc23

### **185067 - Ubuntu Linux 14.04 USN-2824-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-7872

### Description

The scan detected that the host is missing the following update:  
USN-2824-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003205.html>

Ubuntu 14.04

linux-image-3.16.0-55-powerpc-e500mc\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-powerpc64-emb\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-generic\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-generic-lpae\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-lowlatency\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-powerpc-smp\_3.16.0-55.74~14.04.1

linux-image-3.16.0-55-powerpc64-smp\_3.16.0-55.74~14.04.1

### **190050 - Fedora Linux 21 FEDORA-2015-fed35dff7 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5667

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-fed35dff7

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172997.html>

Fedora Core 21



perl-HTML-Scrubber-0.15-1.fc21

### 190052 - Fedora Linux 22 FEDORA-2015-2c155d7632 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5281

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-2c155d7632

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172942.html>

Fedora Core 22

grub2-2.02-0.17.fc22

### 190063 - Fedora Linux 22 FEDORA-2015-95f5ff8d44 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5667

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-95f5ff8d44

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172983.html>

Fedora Core 22

perl-HTML-Scrubber-0.15-1.fc22

### 190065 - Fedora Linux 23 FEDORA-2015-84a95e39d4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5667

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-84a95e39d4

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-November/172934.html>

Fedora Core 23

perl-HTML-Scrubber-0.15-1.fc23

## 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.

### 19019 - (HT205212) Apple iOS Multiple Vulnerabilities Prior To 9

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2013-3951, CVE-2014-8146, CVE-2014-8147, CVE-2014-8611, CVE-2015-0286, CVE-2015-0287, CVE-2015-1129, CVE-2015-1205, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-3801, CVE-2015-5522, CVE-2015-5523, CVE-2015-5748, CVE-2015-5764, CVE-2015-5765, CVE-2015-5767, CVE-2015-5788, CVE-2015-5789, CVE-2015-5790, CVE-2015-5791, CVE-2015-5792, CVE-2015-5793, CVE-2015-5794, CVE-2015-5795, CVE-2015-5796, CVE-2015-5797, CVE-2015-5799, CVE-2015-5800, CVE-2015-5801, CVE-2015-5802, CVE-2015-5803, CVE-2015-5804, CVE-2015-5805, CVE-2015-5806, CVE-2015-5807, CVE-2015-5809, CVE-2015-5810, CVE-2015-5811, CVE-2015-5812, CVE-2015-5813, CVE-2015-5814, CVE-2015-5816, CVE-2015-5817, CVE-2015-5818, CVE-2015-5819, CVE-2015-5820, CVE-2015-5821, CVE-2015-5822, CVE-2015-5823, CVE-2015-5824, CVE-2015-5825, CVE-2015-5826, CVE-2015-5827, CVE-2015-5829, CVE-2015-5831, CVE-2015-5832, CVE-2015-5834, CVE-2015-5835, CVE-2015-5837, CVE-2015-5838, CVE-2015-5839, CVE-2015-5840, CVE-2015-5841, CVE-2015-5842, CVE-2015-5843, CVE-2015-5844, CVE-2015-5845, CVE-2015-5846, CVE-2015-5847, CVE-2015-5848, CVE-2015-5850, CVE-2015-5851, CVE-2015-5855, CVE-2015-5856, CVE-2015-5857, CVE-2015-5858, CVE-2015-5859, CVE-2015-5860, CVE-2015-5861, CVE-2015-5862, CVE-2015-5863, CVE-2015-5867, CVE-2015-5868, CVE-2015-5869, CVE-2015-5874, CVE-2015-5876, CVE-2015-5879, CVE-2015-5880, CVE-2015-5882, CVE-2015-5885, CVE-2015-5892, CVE-2015-5895, CVE-2015-5896, CVE-2015-5898, CVE-2015-5899, CVE-2015-5903, CVE-2015-5904, CVE-2015-5905, CVE-2015-5906, CVE-2015-5907, CVE-2015-5912, CVE-2015-5916, CVE-2015-5921

[Update Details](#)

CVE is updated

### 17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

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

Risk Level: High

CVE: CVE-2014-4113

[Update Details](#)

Risk is updated

### 18858 - (HT205030) Apple iOS Multiple Vulnerabilities Prior To 8.4.1

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2012-6685, CVE-2014-0191, CVE-2014-3660, CVE-2015-3729, CVE-2015-3730, CVE-2015-3731, CVE-2015-3732, CVE-2015-3733, CVE-2015-3734, CVE-2015-3735, CVE-2015-3736, CVE-2015-3737, CVE-2015-3738, CVE-2015-3739, CVE-2015-3740, CVE-2015-3741, CVE-2015-3742, CVE-2015-3743, CVE-2015-3744, CVE-2015-3745, CVE-2015-3746, CVE-2015-3747, CVE-2015-3748, CVE-2015-3749, CVE-2015-3750, CVE-2015-3751, CVE-2015-3752, CVE-2015-3753, CVE-2015-3755, CVE-2015-3756, CVE-2015-3758, CVE-2015-3759, CVE-2015-3763, CVE-2015-3766, CVE-2015-3768, CVE-2015-3776, CVE-2015-3778, CVE-2015-3782, CVE-2015-3784, CVE-2015-3793, CVE-2015-3795, CVE-2015-3796, CVE-2015-3797, CVE-2015-3798, CVE-2015-3800, CVE-2015-

3802, CVE-2015-3803, CVE-2015-3804, CVE-2015-3805, CVE-2015-3806, CVE-2015-3807, CVE-2015-5746, CVE-2015-5749, CVE-2015-5752, CVE-2015-5755, CVE-2015-5756, CVE-2015-5757, CVE-2015-5758, CVE-2015-5759, CVE-2015-5761, CVE-2015-5766, CVE-2015-5769, CVE-2015-5770, CVE-2015-5773, CVE-2015-5774, CVE-2015-5775, CVE-2015-5776, CVE-2015-5777, CVE-2015-5778, CVE-2015-5781, CVE-2015-5782, CVE-2015-5787

#### Update Details

CVE is updated

### **19033 - Avira Management Console Update Manager Service HTTP Header Use-After-Free Remote Code Execution Vulnerability**

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

Risk Level: High

CVE: CVE-2015-7303

#### Update Details

FASLScript is updated

### **19116 - (HT205267) Apple OS X Multiple Vulnerabilities**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-3951, CVE-2014-2532, CVE-2014-3618, CVE-2014-6277, CVE-2014-7186, CVE-2014-7187, CVE-2014-8080, CVE-2014-8090, CVE-2014-8146, CVE-2014-8147, CVE-2014-8611, CVE-2014-9425, CVE-2014-9427, CVE-2014-9652, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232, CVE-2015-0235, CVE-2015-0273, CVE-2015-0286, CVE-2015-0287, CVE-2015-1351, CVE-2015-1352, CVE-2015-1855, CVE-2015-2301, CVE-2015-2305, CVE-2015-2331, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3329, CVE-2015-3330, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-3785, CVE-2015-5522, CVE-2015-5523, CVE-2015-5824, CVE-2015-5830, CVE-2015-5831, CVE-2015-5833, CVE-2015-5836, CVE-2015-5839, CVE-2015-5840, CVE-2015-5841, CVE-2015-5842, CVE-2015-5847, CVE-2015-5849, CVE-2015-5851, CVE-2015-5853, CVE-2015-5854, CVE-2015-5855, CVE-2015-5858, CVE-2015-5859, CVE-2015-5860, CVE-2015-5862, CVE-2015-5863, CVE-2015-5864, CVE-2015-5865, CVE-2015-5866, CVE-2015-5867, CVE-2015-5868, CVE-2015-5869, CVE-2015-5870, CVE-2015-5871, CVE-2015-5872, CVE-2015-5873, CVE-2015-5874, CVE-2015-5875, CVE-2015-5876, CVE-2015-5877, CVE-2015-5878, CVE-2015-5879, CVE-2015-5882, CVE-2015-5883, CVE-2015-5884, CVE-2015-5885, CVE-2015-5887, CVE-2015-5888, CVE-2015-5889, CVE-2015-5890, CVE-2015-5891, CVE-2015-5893, CVE-2015-5894, CVE-2015-5896, CVE-2015-5897, CVE-2015-5899, CVE-2015-5900, CVE-2015-5901, CVE-2015-5902, CVE-2015-5903, CVE-2015-5912, CVE-2015-5913, CVE-2015-5914, CVE-2015-5915, CVE-2015-5917, CVE-2015-5922, CVE-2015-7760

#### Update Details

CVE is updated

### **190025 - Fedora Linux 23 FEDORA-2015-d02feebd15 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-5317, CVE-2015-5318, CVE-2015-5319, CVE-2015-5320, CVE-2015-5321, CVE-2015-5322, CVE-2015-5323, CVE-2015-5324, CVE-2015-5325, CVE-2015-5326

#### Update Details

Risk is updated

### **181283 - FreeBSD Jenkins Slave-originated Arbitrary Code Execution On Master Servers (0dad9114-60cc-11e4-9e84-0022156e8794)**

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

Risk Level: Medium

CVE: CVE-2014-3665

[Update Details](#)

Risk is updated

**189952 - Fedora Linux 22 FEDORA-2015-5062ef3dbe Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5306

[Update Details](#)

Risk is updated

**189985 - Fedora Linux 23 FEDORA-2015-16ecacb90b Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5306

[Update Details](#)

Risk is updated

**18681 - Symantec Endpoint Antivirus Service Is Not Running**

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

**18899 - Symantec Endpoint Antivirus Service Is Installed And Running**

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

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 2015 McAfee, Inc.

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