

## MCAFEE FOUNDSTONE FSL UPDATE

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

### NEW CHECKS

#### 23151 - (HPESBHF03813) HPE Intelligent Management Center Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-8981

#### Description

A vulnerability is present in some versions of HPE Intelligent Management Center.

#### Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A vulnerability is present in some versions of HPE Intelligent Management Center. The flaw is due to a lack of proper validation of user-supplied data's length. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

#### 23170 - Trend Micro Email Encryption Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-6219, CVE-2018-6220, CVE-2018-6221, CVE-2018-6222, CVE-2018-6223, CVE-2018-6224, CVE-2018-6225, CVE-2018-6226, CVE-2018-6227, CVE-2018-6228, CVE-2018-6229, CVE-2018-6230

#### Description

Multiple vulnerabilities are present in some versions of Trend Micro Email Encryption Gateway.

#### Observation

Trend Micro Email Encryption Gateway is a Linux-based product to perform the encryption and decryption of email at the corporate gateway.

Multiple vulnerabilities are present in some versions of Trend Micro Email Encryption Gateway. Successful exploitation could allow an attacker to obtain sensitive information, bypass certain security restrictions, or execute arbitrary code.

#### 146433 - SuSE SLES 11 SP4 SUSE-SU-2018:0555-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1142857, CVE-2017-13215, CVE-2017-17741, CVE-2017-18017, CVE-2017-18079, CVE-2017-5715, CVE-2018-1000004, CVE-2018-5332, CVE-2018-5333

#### Description

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

SUSE-SU-2018:0555-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003756.html>

SuSE SLES 11 SP4

i586

gfs2-kmp-trace-2\_3.0.101\_108.35-0.24.4.6  
kernel-default-base-3.0.101-108.35.1  
kernel-xen-base-3.0.101-108.35.1  
kernel-pae-devel-3.0.101-108.35.1  
cluster-network-kmp-xen-1.4\_3.0.101\_108.35-2.32.4.6  
cluster-network-kmp-trace-1.4\_3.0.101\_108.35-2.32.4.6  
kernel-xen-devel-3.0.101-108.35.1  
gfs2-kmp-default-2\_3.0.101\_108.35-0.24.4.6  
kernel-ec2-3.0.101-108.35.1  
drbd-kmp-default-8.4.4\_3.0.101\_108.35-0.27.4.6  
kernel-source-3.0.101-108.35.1  
kernel-xen-3.0.101-108.35.1  
drbd-8.4.4-0.27.4.2  
ocfs2-kmp-trace-1.6\_3.0.101\_108.35-0.28.5.6  
cluster-network-kmp-default-1.4\_3.0.101\_108.35-2.32.4.6  
gfs2-kmp-pae-2\_3.0.101\_108.35-0.24.4.6  
drbd-udev-8.4.4-0.27.4.2  
cluster-network-kmp-pae-1.4\_3.0.101\_108.35-2.32.4.6  
kernel-pae-3.0.101-108.35.1  
kernel-pae-base-3.0.101-108.35.1  
drbd-pacemaker-8.4.4-0.27.4.2  
drbd-kmp-xen-8.4.4\_3.0.101\_108.35-0.27.4.6  
gfs2-kmp-xen-2\_3.0.101\_108.35-0.24.4.6  
kernel-trace-3.0.101-108.35.1  
drbd-heartbeat-8.4.4-0.27.4.2  
kernel-syms-3.0.101-108.35.1  
ocfs2-kmp-xen-1.6\_3.0.101\_108.35-0.28.5.6  
kernel-default-devel-3.0.101-108.35.1  
drbd-kmp-pae-8.4.4\_3.0.101\_108.35-0.27.4.6  
ocfs2-kmp-pae-1.6\_3.0.101\_108.35-0.28.5.6  
drbd-bash-completion-8.4.4-0.27.4.2  
kernel-ec2-base-3.0.101-108.35.1  
drbd-utils-8.4.4-0.27.4.2  
kernel-ec2-devel-3.0.101-108.35.1  
kernel-trace-base-3.0.101-108.35.1  
ocfs2-kmp-default-1.6\_3.0.101\_108.35-0.28.5.6  
kernel-trace-devel-3.0.101-108.35.1  
drbd-kmp-trace-8.4.4\_3.0.101\_108.35-0.27.4.6  
kernel-default-3.0.101-108.35.1

x86\_64

gfs2-kmp-trace-2\_3.0.101\_108.35-0.24.4.6  
kernel-default-base-3.0.101-108.35.1  
kernel-xen-base-3.0.101-108.35.1  
cluster-network-kmp-xen-1.4\_3.0.101\_108.35-2.32.4.6  
cluster-network-kmp-trace-1.4\_3.0.101\_108.35-2.32.4.6  
kernel-xen-devel-3.0.101-108.35.1  
drbd-kmp-trace-8.4.4\_3.0.101\_108.35-0.27.4.6  
cluster-network-kmp-rt\_trace-1.4\_3.0.101\_rt130\_69.14-2.32.4.6  
drbd-kmp-default-8.4.4\_3.0.101\_108.35-0.27.4.6

kernel-source-3.0.101-108.35.1  
cluster-network-kmp-rt-1.4\_3.0.101\_rt130\_69.14-2.32.4.6  
kernel-xen-3.0.101-108.35.1  
drbd-8.4.4-0.27.4.2  
ocfs2-kmp-trace-1.6\_3.0.101\_108.35-0.28.5.6  
cluster-network-kmp-default-1.4\_3.0.101\_108.35-2.32.4.6  
drbd-udev-8.4.4-0.27.4.2  
drbd-kmp-rt\_trace-8.4.4\_3.0.101\_rt130\_69.14-0.27.4.6  
ocfs2-kmp-rt\_trace-1.6\_3.0.101\_rt130\_69.14-0.28.5.6  
gfs2-kmp-rt-2\_3.0.101\_rt130\_69.14-0.24.4.6  
drbd-kmp-xen-8.4.4\_3.0.101\_108.35-0.27.4.6  
drbd-xen-8.4.4-0.27.4.2  
drbd-pacemaker-8.4.4-0.27.4.2  
drbd-kmp-rt-8.4.4\_3.0.101\_rt130\_69.14-0.27.4.6  
gfs2-kmp-xen-2\_3.0.101\_108.35-0.24.4.6  
kernel-trace-3.0.101-108.35.1  
drbd-heartbeat-8.4.4-0.27.4.2  
kernel-syms-3.0.101-108.35.1  
ocfs2-kmp-xen-1.6\_3.0.101\_108.35-0.28.5.6  
kernel-default-devel-3.0.101-108.35.1  
gfs2-kmp-rt\_trace-2\_3.0.101\_rt130\_69.14-0.24.4.6  
drbd-bash-completion-8.4.4-0.27.4.2  
gfs2-kmp-default-2\_3.0.101\_108.35-0.24.4.6  
kernel-ec2-base-3.0.101-108.35.1  
drbd-utils-8.4.4-0.27.4.2  
kernel-ec2-devel-3.0.101-108.35.1  
kernel-ec2-3.0.101-108.35.1  
kernel-trace-base-3.0.101-108.35.1  
ocfs2-kmp-default-1.6\_3.0.101\_108.35-0.28.5.6  
kernel-trace-devel-3.0.101-108.35.1  
ocfs2-kmp-rt-1.6\_3.0.101\_rt130\_69.14-0.28.5.6  
kernel-default-3.0.101-108.35.1

## 170928 - Amazon Linux AMI ALAS-2018-958 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12374, CVE-2017-12375, CVE-2017-12376, CVE-2017-12377, CVE-2017-12378, CVE-2017-12379, CVE-2017-12380, CVE-2017-6418, CVE-2017-6419, CVE-2017-6420

### Description

The scan detected that the host is missing the following update:  
ALAS-2018-958

### Observation

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

<https://alas.aws.amazon.com/ALAS-2018-958.html>

Amazon Linux AMI

i686  
clamav-milter-0.99.3-1.28.amzn1  
clamav-lib-0.99.3-1.28.amzn1  
clamav-db-0.99.3-1.28.amzn1  
clamav-update-0.99.3-1.28.amzn1  
clamav-0.99.3-1.28.amzn1  
clamd-0.99.3-1.28.amzn1

clamav-devel-0.99.3-1.28.amzn1  
clamav-server-0.99.3-1.28.amzn1  
clamav-debuginfo-0.99.3-1.28.amzn1

noarch

clamav-data-0.99.3-1.28.amzn1  
clamav-data-empty-0.99.3-1.28.amzn1  
clamav-milter-sysvinit-0.99.3-1.28.amzn1  
clamav-scanner-0.99.3-1.28.amzn1  
clamav-filesystem-0.99.3-1.28.amzn1  
clamav-scanner-sysvinit-0.99.3-1.28.amzn1  
clamav-server-sysvinit-0.99.3-1.28.amzn1

x86\_64

clamav-milter-0.99.3-1.28.amzn1  
clamav-lib-0.99.3-1.28.amzn1  
clamav-db-0.99.3-1.28.amzn1  
clamav-update-0.99.3-1.28.amzn1  
clamav-0.99.3-1.28.amzn1  
clamd-0.99.3-1.28.amzn1  
clamav-devel-0.99.3-1.28.amzn1  
clamav-server-0.99.3-1.28.amzn1  
clamav-debuginfo-0.99.3-1.28.amzn1

## 186112 - Ubuntu Linux 14.04 USN-3583-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0750, CVE-2017-0861, CVE-2017-1000407, CVE-2017-12153, CVE-2017-12190, CVE-2017-12192, CVE-2017-14051, CVE-2017-14140, CVE-2017-14156, CVE-2017-14489, CVE-2017-15102, CVE-2017-15115, CVE-2017-15274, CVE-2017-15868, CVE-2017-16525, CVE-2017-17450, CVE-2017-17806, CVE-2017-18017, CVE-2017-5669, CVE-2017-5754, CVE-2017-7542, CVE-2017-7889, CVE-2017-8824, CVE-2018-5333, CVE-2018-5344

### Description

The scan detected that the host is missing the following update:  
USN-3583-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004296.html>

Ubuntu 14.04

linux-image-powerpc64-smp\_3.13.0.142.152  
linux-image-generic\_3.13.0.142.152  
linux-image-3.13.0-142-powerpc-smp\_3.13.0-142.191  
linux-image-3.13.0-142-lowlatency\_3.13.0-142.191  
linux-image-powerpc-e500\_3.13.0.142.152  
linux-image-3.13.0-142-powerpc64-smp\_3.13.0-142.191  
linux-image-powerpc-e500mc\_3.13.0.142.152  
linux-image-3.13.0-142-powerpc-e500mc\_3.13.0-142.191  
linux-image-3.13.0-142-powerpc-e500\_3.13.0-142.191  
linux-image-3.13.0-142-generic-lpae\_3.13.0-142.191  
linux-image-powerpc-smp\_3.13.0.142.152  
linux-image-lowlatency\_3.13.0.142.152  
linux-image-powerpc64-emb\_3.13.0.142.152

linux-image-3.13.0-142-generic\_3.13.0-142.191  
linux-image-generic-lpae\_3.13.0.142.152  
linux-image-3.13.0-142-powerpc64-emb\_3.13.0-142.191

## 186117 - Ubuntu Linux 12.04 USN-3583-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-0750, CVE-2017-0861, CVE-2017-1000407, CVE-2017-12153, CVE-2017-12190, CVE-2017-12192, CVE-2017-14051, CVE-2017-14140, CVE-2017-14156, CVE-2017-14489, CVE-2017-15102, CVE-2017-15115, CVE-2017-15274, CVE-2017-15868, CVE-2017-16525, CVE-2017-17450, CVE-2017-17806, CVE-2017-18017, CVE-2017-5669, CVE-2017-7542, CVE-2017-7889, CVE-2017-8824, CVE-2018-5333, CVE-2018-5344

### Description

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

USN-3583-2

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004297.html>

Ubuntu 12.04

linux-image-3.13.0-142-generic-lpae\_3.13.0-142.191~precise1

linux-image-generic-lts-trusty\_3.13.0.142.133

linux-image-3.13.0-142-generic\_3.13.0-142.191~precise1

linux-image-generic-lpae-lts-trusty\_3.13.0.142.133

## 23158 - (HPESBHF03808) HPE Intelligent Management Center Remote Code Execution Vulnerability

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8983

### Description

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center.

### Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in how the software handle objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

## 23126 - IBM AIX Aixbase Multiple Vulnerabilities (aixbase\_advisory)

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

Risk Level: High

CVE: CVE-2018-1383

### Description

A vulnerability is present in some versions of IBM AIX.

#### Observation

AIX is an Unix-like operating system developed by IBM.

A vulnerability is present in some versions of IBM AIX. The flaw is unspecified. Successful exploitation could allow an attacker with root privileges on one system to obtain root access on another machine.

### 23155 - Oracle Identity Manager Default Account Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-10151

#### Description

A vulnerability is present in some versions of Oracle Identity Manager.

#### Observation

Oracle Identity Manager is an enterprise software suite that provides identity and access management.

A vulnerability is present in some versions of Oracle Identity Manager. The flaw lies in the subcomponent default account. Successful exploitation could allow a remote attacker to take complete control of Oracle Identity Manager.

### 23163 - (HT208534) Apple iOS Vulnerability Prior To 11.2.6

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2018-4124

#### Description

A vulnerability is present in some versions of Apple iOS.

#### Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

A vulnerability is present in some versions of Apple iOS. The flaw lies in CoreText component. Successful exploitation could allow an attacker to cause a heap corruption.

### 23128 - IBM AIX Suid Multiple Vulnerabilities (suid\_advisory)

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

Risk Level: High

CVE: CVE-2017-1692

#### Description

Multiple vulnerabilities are present in some versions of IBM AIX.

#### Observation

AIX is a Unix-like operating system developed by IBM.

Multiple vulnerabilities are present in some versions of IBM AIX. The flaws lie in bellmail, caccelstat, iostat, lquerypv, restbyinode, and vmstat. Successful exploitation could allow a local attacker to gain root privileges.

## 23134 - (VMSA-2018-0006) VMware vSphere Integrated Containers Deserialization Vulnerability

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

Risk Level: High

CVE: CVE-2017-4947

### Description

A vulnerability is present in some versions of VMware vSphere Integrated Containers.

### Observation

VMware vSphere Integrated Container (VIC) is a platform that helps to deploy and manage containers within virtual machines.

A vulnerability is present in some versions of VMware vSphere Integrated Containers. The flaw is due to deserialization via Xenon. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

## 23137 - PostgreSQL Multiple Vulnerabilities (Feb 2018)

Category: General Vulnerability Assessment -> NonIntrusive -> Potentially Vulnerable

Risk Level: High

CVE: CVE-2018-1052, CVE-2018-1053

### Description

Multiple vulnerabilities are present in some versions of PostgreSQL.

### Observation

PostgreSQL is an open-source object-relational database management system.

Multiple vulnerabilities are present in some versions of PostgreSQL. The flaws lie in multiple components. Successful exploitation could allow an attacker to bypass security measure or retrieve sensitive data.

## 23145 - Gemalto Sentinel License Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-11496, CVE-2017-11497, CVE-2017-11498, CVE-2017-12818, CVE-2017-12820, CVE-2017-12821, CVE-2017-12822

### Description

Multiple vulnerabilities are present in some versions of Gemalto Sentinel License Manager.

### Observation

Gemalto Sentinel License Manager is a licensing solution for software and technology.

Multiple vulnerabilities are present in some versions of Gemalto Sentinel License Manager. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code or cause denial of service condition.

## 23146 - IBM WebSphere Portal Apache Commons FileUpload Vulnerability (swg22012419)

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

Risk Level: High

CVE: CVE-2016-1000031

### Description

Remote code execution vulnerability is present in some versions of IBM WebSphere Portal.

### Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

Remote code execution vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in deserialization of untrusted data in DiskFileItem class of the FileUpload library. Successful exploitation could allow an attacker to execute arbitrary code in the context of the current process.

## 23150 - (HPESBHF03815) HPE Intelligent Management Center Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-5792

### Description

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center.

### Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

A remote code execution vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in RMI Registry and is due to improper validation of user supplied data. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

## 23157 - (SB10224) McAfee Application and Change Control Authentication Bypass Vulnerability

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

Risk Level: High

CVE: CVE-2017-3912

### Description

A vulnerability is present in some versions of McAfee Application and Change Control.

### Observation

McAfee Application and Change Control is a commercial file integrity monitoring solution for Windows systems.

A vulnerability is present in some versions of McAfee Application and Change Control. The flaw lies in a command-line utility. Successful exploitation could allow an authenticated attacker to bypass password security.

## 23160 - IBM WebSphere Portal Apache POI Denial Of Service Vulnerability (swg22008072)

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

Risk Level: High

CVE: CVE-2017-5644

### Description



A Denial-of-Service vulnerability is present in some versions of IBM WebSphere Portal.

#### Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

A Denial-of-Service vulnerability is present in some versions of IBM WebSphere Portal. The flaw lies in how the Apache POI component handles XML data. Successful exploitation could allow an attacker to cause a denial of service. Exploitation requires a malicious user to send a specially-crafted OOXML file.

### 131028 - Debian Linux 8.0, 9.0 DSA-4124-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629, CVE-2017-3163

#### Description

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

DSA-4124-1

#### Observation

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

For more information see:

<http://www.debian.org/security/2018/dsa-4124>

Debian 8.0

all

solr-common\_3.6.2+dfsg-5+deb8u1

liblucene3-java\_3.6.2+dfsg-5+deb8u1

solr-jetty\_3.6.2+dfsg-5+deb8u1

liblucene3-java-doc\_3.6.2+dfsg-5+deb8u1

solr-tomcat\_3.6.2+dfsg-5+deb8u1

libsolr-java\_3.6.2+dfsg-5+deb8u1

liblucene3-contrib-java\_3.6.2+dfsg-5+deb8u1

Debian 9.0

all

solr-tomcat\_3.6.2+dfsg-10+deb9u1

libsolr-java\_3.6.2+dfsg-10+deb9u1

liblucene3-java\_3.6.2+dfsg-10+deb9u1

solr-jetty\_3.6.2+dfsg-10+deb9u1

liblucene3-java-doc\_3.6.2+dfsg-10+deb9u1

solr-common\_3.6.2+dfsg-10+deb9u1

liblucene3-contrib-java\_3.6.2+dfsg-10+deb9u1

### 141873 - Red Hat Enterprise Linux RHSA-2018-0342 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-17485, CVE-2017-7525

#### Description

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

RHSA-2018-0342

## Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-February/msg00022.html>

## RHEL7S

noarch  
rh-maven35-jackson-databind-2.7.6-2.4.el7  
rh-maven35-jackson-databind-javadoc-2.7.6-2.4.el7

## RHEL7WS

noarch  
rh-maven35-jackson-databind-2.7.6-2.4.el7  
rh-maven35-jackson-databind-javadoc-2.7.6-2.4.el7

## RHEL7\_3S

noarch  
rh-maven35-jackson-databind-2.7.6-2.4.el7  
rh-maven35-jackson-databind-javadoc-2.7.6-2.4.el7

## 146422 - SuSE Linux 42.3 openSUSE-SU-2018:0520-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0520-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00091.html>

## SuSE Linux 42.3

i586  
db48-utils-4.8.30-34.3.1  
libdb\_java-4\_8-4.8.30-34.3.1  
libdb-4\_8-4.8.30-34.3.1  
libdb\_java-4\_8-devel-4.8.30-34.3.1  
libdb\_java-4\_8-debugsource-4.8.30-34.3.1  
libdb-4\_8-debugsource-4.8.30-34.3.1  
libdb-4\_8-devel-4.8.30-34.3.1  
libdb-4\_8-debuginfo-4.8.30-34.3.1  
libdb\_java-4\_8-debuginfo-4.8.30-34.3.1

## noarch

db48-doc-4.8.30-34.3.1

## x86\_64

db48-utils-4.8.30-34.3.1  
libdb\_java-4\_8-4.8.30-34.3.1  
libdb-4\_8-4.8.30-34.3.1  
libdb\_java-4\_8-devel-4.8.30-34.3.1  
libdb\_java-4\_8-debugsource-4.8.30-34.3.1

libdb-4\_8-debugsource-4.8.30-34.3.1  
libdb-4\_8-devel-4.8.30-34.3.1  
libdb-4\_8-32bit-4.8.30-34.3.1  
libdb-4\_8-debuginfo-4.8.30-34.3.1  
libdb\_java-4\_8-debuginfo-4.8.30-34.3.1  
libdb-4\_8-debuginfo-32bit-4.8.30-34.3.1  
libdb-4\_8-devel-32bit-4.8.30-34.3.1

## 146423 - SuSE Linux 42.3 openSUSE-SU-2018:0523-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1053

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0523-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00094.html>

SuSE Linux 42.3

i586

postgresql96-server-9.6.7-12.1  
libecpg6-9.6.7-12.1  
postgresql96-devel-9.6.7-12.1  
postgresql96-contrib-9.6.7-12.1  
postgresql96-devel-debuginfo-9.6.7-12.1  
postgresql96-debugsource-9.6.7-12.1  
libpq5-debuginfo-9.6.7-12.1  
postgresql96-plpython-9.6.7-12.1  
postgresql96-plperl-9.6.7-12.1  
postgresql96-test-9.6.7-12.1  
postgresql96-plpython-debuginfo-9.6.7-12.1  
postgresql96-server-debuginfo-9.6.7-12.1  
postgresql96-contrib-debuginfo-9.6.7-12.1  
postgresql96-plperl-debuginfo-9.6.7-12.1  
postgresql96-libs-debugsource-9.6.7-12.1  
postgresql96-pltcl-9.6.7-12.1  
libpq5-9.6.7-12.1  
postgresql96-pltcl-debuginfo-9.6.7-12.1  
postgresql96-9.6.7-12.1  
libecpg6-debuginfo-9.6.7-12.1  
postgresql96-debuginfo-9.6.7-12.1

noarch

postgresql96-docs-9.6.7-12.1

x86\_64

postgresql96-server-9.6.7-12.1  
libecpg6-9.6.7-12.1  
postgresql96-devel-9.6.7-12.1  
postgresql96-contrib-9.6.7-12.1  
postgresql96-devel-debuginfo-9.6.7-12.1  
postgresql96-debugsource-9.6.7-12.1

libpq5-debuginfo-9.6.7-12.1  
postgresql96-plpython-9.6.7-12.1  
postgresql96-plperl-9.6.7-12.1  
postgresql96-test-9.6.7-12.1  
postgresql96-plpython-debuginfo-9.6.7-12.1  
postgresql96-server-debuginfo-9.6.7-12.1  
libpq5-debuginfo-32bit-9.6.7-12.1  
postgresql96-contrib-debuginfo-9.6.7-12.1  
postgresql96-plperl-debuginfo-9.6.7-12.1  
postgresql96-libs-debugsource-9.6.7-12.1  
postgresql96-pltcl-9.6.7-12.1  
libpq5-9.6.7-12.1  
postgresql96-pltcl-debuginfo-9.6.7-12.1  
libecpg6-debuginfo-32bit-9.6.7-12.1  
postgresql96-9.6.7-12.1  
libecpg6-debuginfo-9.6.7-12.1  
postgresql96-debuginfo-9.6.7-12.1  
libecpg6-32bit-9.6.7-12.1  
libpq5-32bit-9.6.7-12.1

## 146424 - SuSE Linux 42.3 openSUSE-SU-2018:0540-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7320, CVE-2018-7321, CVE-2018-7322, CVE-2018-7323, CVE-2018-7324, CVE-2018-7325, CVE-2018-7326, CVE-2018-7327, CVE-2018-7328, CVE-2018-7329, CVE-2018-7330, CVE-2018-7331, CVE-2018-7332, CVE-2018-7333, CVE-2018-7334, CVE-2018-7335, CVE-2018-7336, CVE-2018-7337, CVE-2018-7417, CVE-2018-7418, CVE-2018-7419, CVE-2018-7420, CVE-2018-7421

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0540-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00104.html>

SuSE Linux 42.3

x86\_64

wireshark-ui-qt-debuginfo-2.2.13-35.1  
wireshark-2.2.13-35.1  
wireshark-ui-qt-2.2.13-35.1  
wireshark-debuginfo-2.2.13-35.1  
wireshark-ui-gtk-debuginfo-2.2.13-35.1  
wireshark-ui-gtk-2.2.13-35.1  
wireshark-devel-2.2.13-35.1  
wireshark-debugsource-2.2.13-35.1

## 146426 - SuSE Linux 42.3 openSUSE-SU-2018:0542-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11533, CVE-2017-17500, CVE-2017-17682

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0542-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00106.html>

SuSE Linux 42.3

x86\_64

libGraphicsMagick-Q16-3-debuginfo-1.3.25-74.1  
perl-GraphicsMagick-debuginfo-1.3.25-74.1  
libGraphicsMagick-Q16-3-1.3.25-74.1  
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-74.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-74.1  
libGraphicsMagickWand-Q16-2-1.3.25-74.1  
libGraphicsMagick++-devel-1.3.25-74.1  
perl-GraphicsMagick-1.3.25-74.1  
GraphicsMagick-1.3.25-74.1  
GraphicsMagick-debugsource-1.3.25-74.1  
libGraphicsMagick++-Q16-12-1.3.25-74.1  
GraphicsMagick-devel-1.3.25-74.1  
libGraphicsMagick3-config-1.3.25-74.1  
GraphicsMagick-debuginfo-1.3.25-74.1

i586

libGraphicsMagick-Q16-3-debuginfo-1.3.25-74.1  
perl-GraphicsMagick-debuginfo-1.3.25-74.1  
libGraphicsMagick-Q16-3-1.3.25-74.1  
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-74.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-74.1  
libGraphicsMagickWand-Q16-2-1.3.25-74.1  
libGraphicsMagick++-devel-1.3.25-74.1  
perl-GraphicsMagick-1.3.25-74.1  
GraphicsMagick-1.3.25-74.1  
GraphicsMagick-debugsource-1.3.25-74.1  
libGraphicsMagick++-Q16-12-1.3.25-74.1  
GraphicsMagick-devel-1.3.25-74.1  
libGraphicsMagick3-config-1.3.25-74.1  
GraphicsMagick-debuginfo-1.3.25-74.1

146427 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0532-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3144

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2018:0532-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003752.html>

SuSE SLES 12 SP2

x86\_64

dhcp-4.3.3-10.11.1

dhcp-relay-debuginfo-4.3.3-10.11.1

dhcp-client-debuginfo-4.3.3-10.11.1

dhcp-server-debuginfo-4.3.3-10.11.1

dhcp-debugsource-4.3.3-10.11.1

dhcp-relay-4.3.3-10.11.1

dhcp-client-4.3.3-10.11.1

dhcp-server-4.3.3-10.11.1

dhcp-debuginfo-4.3.3-10.11.1

SuSE SLED 12 SP3

x86\_64

dhcp-4.3.3-10.11.1

dhcp-client-debuginfo-4.3.3-10.11.1

dhcp-client-4.3.3-10.11.1

dhcp-debuginfo-4.3.3-10.11.1

dhcp-debugsource-4.3.3-10.11.1

SuSE SLED 12 SP2

x86\_64

dhcp-4.3.3-10.11.1

dhcp-client-debuginfo-4.3.3-10.11.1

dhcp-client-4.3.3-10.11.1

dhcp-debuginfo-4.3.3-10.11.1

dhcp-debugsource-4.3.3-10.11.1

SuSE SLES 12 SP3

x86\_64

dhcp-4.3.3-10.11.1

dhcp-relay-debuginfo-4.3.3-10.11.1

dhcp-client-debuginfo-4.3.3-10.11.1

dhcp-server-debuginfo-4.3.3-10.11.1

dhcp-debugsource-4.3.3-10.11.1

dhcp-relay-4.3.3-10.11.1

dhcp-client-4.3.3-10.11.1

dhcp-server-4.3.3-10.11.1

dhcp-debuginfo-4.3.3-10.11.1

## 146430 - SuSE Linux 42.3 openSUSE-SU-2018:0538-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10712

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0538-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00102.html>

SuSE Linux 42.3

i586

php5-gd-debuginfo-5.5.14-94.1  
php5-ldap-5.5.14-94.1  
php5-ftp-5.5.14-94.1  
php5-snmp-debuginfo-5.5.14-94.1  
php5-iconv-debuginfo-5.5.14-94.1  
php5-dba-5.5.14-94.1  
php5-mysql-debuginfo-5.5.14-94.1  
php5-xsl-5.5.14-94.1  
php5-readline-5.5.14-94.1  
php5-zip-5.5.14-94.1  
php5-pdo-5.5.14-94.1  
php5-sysvsem-debuginfo-5.5.14-94.1  
php5-gd-5.5.14-94.1  
php5-sockets-5.5.14-94.1  
php5-fpm-debuginfo-5.5.14-94.1  
php5-pgsql-debuginfo-5.5.14-94.1  
php5-firebird-debuginfo-5.5.14-94.1  
php5-sqlite-debuginfo-5.5.14-94.1  
php5-posix-debuginfo-5.5.14-94.1  
php5-sysvshm-5.5.14-94.1  
php5-shmop-debuginfo-5.5.14-94.1  
php5-devel-5.5.14-94.1  
php5-xmlwriter-debuginfo-5.5.14-94.1  
php5-fpm-5.5.14-94.1  
php5-dba-debuginfo-5.5.14-94.1  
php5-json-5.5.14-94.1  
php5-pcntl-5.5.14-94.1  
php5-xmlreader-debuginfo-5.5.14-94.1  
php5-iconv-5.5.14-94.1  
php5-shmop-5.5.14-94.1  
php5-5.5.14-94.1  
php5-debuginfo-5.5.14-94.1  
php5-bz2-5.5.14-94.1  
php5-sockets-debuginfo-5.5.14-94.1  
php5-debugsource-5.5.14-94.1  
php5-soap-debuginfo-5.5.14-94.1  
php5-snmp-5.5.14-94.1  
php5-mssql-debuginfo-5.5.14-94.1  
php5-fastcgi-debuginfo-5.5.14-94.1  
php5-mbstring-5.5.14-94.1  
php5-gmp-debuginfo-5.5.14-94.1  
php5-posix-5.5.14-94.1  
php5-pspell-debuginfo-5.5.14-94.1  
php5-opcache-5.5.14-94.1  
php5-enchanted-5.5.14-94.1  
php5-sysvsem-5.5.14-94.1  
php5-curl-5.5.14-94.1  
php5-pgsql-5.5.14-94.1  
php5-odbc-debuginfo-5.5.14-94.1  
php5-pdo-debuginfo-5.5.14-94.1  
php5-ctype-debuginfo-5.5.14-94.1  
php5-curl-debuginfo-5.5.14-94.1  
php5-xmlrpc-5.5.14-94.1  
php5-tidy-debuginfo-5.5.14-94.1  
php5-intl-5.5.14-94.1  
php5-wddx-5.5.14-94.1  
php5-fileinfo-5.5.14-94.1  
php5-gmp-5.5.14-94.1  
php5-zlib-5.5.14-94.1

php5-soap-5.5.14-94.1  
php5-calendar-5.5.14-94.1  
php5-bz2-debuginfo-5.5.14-94.1  
php5-enchanted-debuginfo-5.5.14-94.1  
php5-sysvmsg-5.5.14-94.1  
php5-openssl-5.5.14-94.1  
php5-suhosin-debuginfo-5.5.14-94.1  
php5-opcache-debuginfo-5.5.14-94.1  
php5-pcntl-debuginfo-5.5.14-94.1  
php5-zlib-debuginfo-5.5.14-94.1  
php5-mcrypt-5.5.14-94.1  
php5-ldap-debuginfo-5.5.14-94.1  
php5-json-debuginfo-5.5.14-94.1  
php5-phar-debuginfo-5.5.14-94.1  
php5-firebird-5.5.14-94.1  
php5-pspell-5.5.14-94.1  
php5-tokenizer-5.5.14-94.1  
php5-intl-debuginfo-5.5.14-94.1  
php5-xsl-debuginfo-5.5.14-94.1  
php5-calendar-debuginfo-5.5.14-94.1  
apache2-mod\_php5-5.5.14-94.1  
php5-tidy-5.5.14-94.1  
php5-ctype-5.5.14-94.1  
php5-fileinfo-debuginfo-5.5.14-94.1  
php5-mbstring-debuginfo-5.5.14-94.1  
php5-exif-debuginfo-5.5.14-94.1  
php5-tokenizer-debuginfo-5.5.14-94.1  
php5-exif-5.5.14-94.1  
php5-sqlite-5.5.14-94.1  
php5-ldap-5.5.14-94.1  
php5-gettext-debuginfo-5.5.14-94.1  
php5-bcmath-5.5.14-94.1  
php5-ldap-debuginfo-5.5.14-94.1  
php5-zip-debuginfo-5.5.14-94.1  
php5-phar-5.5.14-94.1  
php5-bcmath-debuginfo-5.5.14-94.1  
php5-xmlrpc-debuginfo-5.5.14-94.1  
php5-xmlwriter-5.5.14-94.1  
php5-xmlreader-5.5.14-94.1  
apache2-mod\_php5-debuginfo-5.5.14-94.1  
php5-mysql-5.5.14-94.1  
php5-suhosin-5.5.14-94.1  
php5-ftp-debuginfo-5.5.14-94.1  
php5-fastcgi-5.5.14-94.1  
php5-sysvmsg-debuginfo-5.5.14-94.1  
php5-gettext-5.5.14-94.1  
php5-wddx-debuginfo-5.5.14-94.1  
php5-sysvshm-debuginfo-5.5.14-94.1  
php5-dom-debuginfo-5.5.14-94.1  
php5-dom-5.5.14-94.1  
php5-openssl-debuginfo-5.5.14-94.1  
php5-readline-debuginfo-5.5.14-94.1  
php5-mcrypt-debuginfo-5.5.14-94.1  
php5-odbc-5.5.14-94.1  
php5-mysql-5.5.14-94.1

noarch

php5-pear-5.5.14-94.1

x86\_64



php5-gd-debuginfo-5.5.14-94.1  
php5-ldap-5.5.14-94.1  
php5-ftp-5.5.14-94.1  
php5-snmp-debuginfo-5.5.14-94.1  
php5-iconv-debuginfo-5.5.14-94.1  
php5-dba-5.5.14-94.1  
php5-mysql-debuginfo-5.5.14-94.1  
php5-xsl-5.5.14-94.1  
php5-readline-5.5.14-94.1  
php5-zip-5.5.14-94.1  
php5-pdo-5.5.14-94.1  
php5-sysvsem-debuginfo-5.5.14-94.1  
php5-gd-5.5.14-94.1  
php5-sockets-5.5.14-94.1  
php5-fpm-debuginfo-5.5.14-94.1  
php5-pgsql-debuginfo-5.5.14-94.1  
php5-firebird-debuginfo-5.5.14-94.1  
php5-sqlite-debuginfo-5.5.14-94.1  
php5-posix-debuginfo-5.5.14-94.1  
php5-sysvshm-5.5.14-94.1  
php5-shmop-debuginfo-5.5.14-94.1  
php5-devel-5.5.14-94.1  
php5-xmlwriter-debuginfo-5.5.14-94.1  
php5-fpm-5.5.14-94.1  
php5-dba-debuginfo-5.5.14-94.1  
php5-json-5.5.14-94.1  
php5-pcntl-5.5.14-94.1  
php5-xmlreader-debuginfo-5.5.14-94.1  
php5-iconv-5.5.14-94.1  
php5-shmop-5.5.14-94.1  
php5-5.5.14-94.1  
php5-debuginfo-5.5.14-94.1  
php5-bz2-5.5.14-94.1  
php5-sockets-debuginfo-5.5.14-94.1  
php5-debugsource-5.5.14-94.1  
php5-soap-debuginfo-5.5.14-94.1  
php5-snmp-5.5.14-94.1  
php5-mssql-debuginfo-5.5.14-94.1  
php5-fastcgi-debuginfo-5.5.14-94.1  
php5-mbstring-5.5.14-94.1  
php5-gmp-debuginfo-5.5.14-94.1  
php5-posix-5.5.14-94.1  
php5-pspell-debuginfo-5.5.14-94.1  
php5-opcache-5.5.14-94.1  
php5-enchanted-5.5.14-94.1  
php5-sysvsem-5.5.14-94.1  
php5-curl-5.5.14-94.1  
php5-pgsql-5.5.14-94.1  
php5-odbc-debuginfo-5.5.14-94.1  
php5-pdo-debuginfo-5.5.14-94.1  
php5-ctype-debuginfo-5.5.14-94.1  
php5-curl-debuginfo-5.5.14-94.1  
php5-xmlrpc-5.5.14-94.1  
php5-tidy-debuginfo-5.5.14-94.1  
php5-intl-5.5.14-94.1  
php5-wddx-5.5.14-94.1  
php5-fileinfo-5.5.14-94.1  
php5-gmp-5.5.14-94.1  
php5-zlib-5.5.14-94.1  
php5-soap-5.5.14-94.1

php5-calendar-5.5.14-94.1  
php5-bz2-debuginfo-5.5.14-94.1  
php5-enchanted-debuginfo-5.5.14-94.1  
php5-sysvmsg-5.5.14-94.1  
php5-openssl-5.5.14-94.1  
php5-suhosin-debuginfo-5.5.14-94.1  
php5-opcache-debuginfo-5.5.14-94.1  
php5-pcntl-debuginfo-5.5.14-94.1  
php5-zlib-debuginfo-5.5.14-94.1  
php5-mcrypt-5.5.14-94.1  
php5-imap-debuginfo-5.5.14-94.1  
php5-json-debuginfo-5.5.14-94.1  
php5-phar-debuginfo-5.5.14-94.1  
php5-firebird-5.5.14-94.1  
php5-pspell-5.5.14-94.1  
php5-tokenizer-5.5.14-94.1  
php5-intl-debuginfo-5.5.14-94.1  
php5-xsl-debuginfo-5.5.14-94.1  
php5-calendar-debuginfo-5.5.14-94.1  
apache2-mod\_php5-5.5.14-94.1  
php5-tidy-5.5.14-94.1  
php5-ctype-5.5.14-94.1  
php5-fileinfo-debuginfo-5.5.14-94.1  
php5-mbstring-debuginfo-5.5.14-94.1  
php5-exif-debuginfo-5.5.14-94.1  
php5-tokenizer-debuginfo-5.5.14-94.1  
php5-exif-5.5.14-94.1  
php5-sqlite-5.5.14-94.1  
php5-imap-5.5.14-94.1  
php5-gettext-debuginfo-5.5.14-94.1  
php5-bcmath-5.5.14-94.1  
php5-ldap-debuginfo-5.5.14-94.1  
php5-zip-debuginfo-5.5.14-94.1  
php5-phar-5.5.14-94.1  
php5-bcmath-debuginfo-5.5.14-94.1  
php5-xmlrpc-debuginfo-5.5.14-94.1  
php5-xmlwriter-5.5.14-94.1  
php5-xmlreader-5.5.14-94.1  
apache2-mod\_php5-debuginfo-5.5.14-94.1  
php5-mssql-5.5.14-94.1  
php5-suhosin-5.5.14-94.1  
php5-ftp-debuginfo-5.5.14-94.1  
php5-fastcgi-5.5.14-94.1  
php5-sysvmsg-debuginfo-5.5.14-94.1  
php5-gettext-5.5.14-94.1  
php5-wddx-debuginfo-5.5.14-94.1  
php5-sysvshm-debuginfo-5.5.14-94.1  
php5-dom-debuginfo-5.5.14-94.1  
php5-dom-5.5.14-94.1  
php5-openssl-debuginfo-5.5.14-94.1  
php5-readline-debuginfo-5.5.14-94.1  
php5-mcrypt-debuginfo-5.5.14-94.1  
php5-odbc-5.5.14-94.1  
php5-mysql-5.5.14-94.1

146432 - SuSE Linux 42.3 openSUSE-SU-2018:0529-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15098, CVE-2017-15099, CVE-2017-7546, CVE-2017-7547, CVE-2017-7548, CVE-2018-1053

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0529-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00097.html>

SuSE Linux 42.3

i586

postgresql95-server-9.5.11-2.3.1  
postgresql95-plpython-debuginfo-9.5.11-2.3.1  
postgresql95-libs-debugsource-9.5.11-2.3.1  
postgresql95-server-debuginfo-9.5.11-2.3.1  
postgresql95-contrib-9.5.11-2.3.1  
postgresql95-debugsource-9.5.11-2.3.1  
postgresql95-plpython-9.5.11-2.3.1  
postgresql95-plperl-9.5.11-2.3.1  
postgresql95-contrib-debuginfo-9.5.11-2.3.1  
postgresql95-devel-9.5.11-2.3.1  
postgresql95-pltcl-9.5.11-2.3.1  
postgresql95-debuginfo-9.5.11-2.3.1  
postgresql95-test-9.5.11-2.3.1  
postgresql95-pltcl-debuginfo-9.5.11-2.3.1  
postgresql95-devel-debuginfo-9.5.11-2.3.1  
postgresql95-plperl-debuginfo-9.5.11-2.3.1  
postgresql95-9.5.11-2.3.1

noarch

postgresql95-docs-9.5.11-2.3.1

x86\_64

postgresql95-server-9.5.11-2.3.1  
postgresql95-plpython-debuginfo-9.5.11-2.3.1  
postgresql95-libs-debugsource-9.5.11-2.3.1  
postgresql95-server-debuginfo-9.5.11-2.3.1  
postgresql95-contrib-9.5.11-2.3.1  
postgresql95-debugsource-9.5.11-2.3.1  
postgresql95-plpython-9.5.11-2.3.1  
postgresql95-plperl-9.5.11-2.3.1  
postgresql95-contrib-debuginfo-9.5.11-2.3.1  
postgresql95-devel-9.5.11-2.3.1  
postgresql95-pltcl-9.5.11-2.3.1  
postgresql95-debuginfo-9.5.11-2.3.1  
postgresql95-test-9.5.11-2.3.1  
postgresql95-pltcl-debuginfo-9.5.11-2.3.1  
postgresql95-devel-debuginfo-9.5.11-2.3.1  
postgresql95-plperl-debuginfo-9.5.11-2.3.1  
postgresql95-9.5.11-2.3.1

146435 - SuSE Linux 42.3 openSUSE-SU-2018:0537-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3144

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0537-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00101.html>

SuSE Linux 42.3

x86\_64

dhcp-relay-4.3.3-11.3.1

dhcp-devel-4.3.3-11.3.1

dhcp-debugsource-4.3.3-11.3.1

dhcp-client-4.3.3-11.3.1

dhcp-debuginfo-4.3.3-11.3.1

dhcp-server-4.3.3-11.3.1

dhcp-relay-debuginfo-4.3.3-11.3.1

dhcp-doc-4.3.3-11.3.1

dhcp-4.3.3-11.3.1

dhcp-client-debuginfo-4.3.3-11.3.1

dhcp-server-debuginfo-4.3.3-11.3.1

i586

dhcp-relay-4.3.3-11.3.1

dhcp-devel-4.3.3-11.3.1

dhcp-debugsource-4.3.3-11.3.1

dhcp-client-4.3.3-11.3.1

dhcp-debuginfo-4.3.3-11.3.1

dhcp-server-4.3.3-11.3.1

dhcp-relay-debuginfo-4.3.3-11.3.1

dhcp-doc-4.3.3-11.3.1

dhcp-4.3.3-11.3.1

dhcp-client-debuginfo-4.3.3-11.3.1

dhcp-server-debuginfo-4.3.3-11.3.1

146436 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0510-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2018:0510-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003748.html>

SuSE SLES 12 SP2

x86\_64

libdb-4\_8-32bit-4.8.30-29.6  
libdb-4\_8-debuginfo-4.8.30-29.6  
libdb-4\_8-debugsource-4.8.30-29.6  
db48-utils-4.8.30-29.6  
libdb-4\_8-4.8.30-29.6  
libdb-4\_8-debuginfo-32bit-4.8.30-29.6

SuSE SLED 12 SP3

x86\_64  
libdb-4\_8-32bit-4.8.30-29.6  
libdb-4\_8-debuginfo-4.8.30-29.6  
libdb-4\_8-debugsource-4.8.30-29.6  
db48-utils-4.8.30-29.6  
libdb-4\_8-4.8.30-29.6  
libdb-4\_8-debuginfo-32bit-4.8.30-29.6

SuSE SLED 12 SP2

x86\_64  
libdb-4\_8-32bit-4.8.30-29.6  
libdb-4\_8-debuginfo-4.8.30-29.6  
libdb-4\_8-debugsource-4.8.30-29.6  
db48-utils-4.8.30-29.6  
libdb-4\_8-4.8.30-29.6  
libdb-4\_8-debuginfo-32bit-4.8.30-29.6

SuSE SLES 12 SP3

x86\_64  
libdb-4\_8-32bit-4.8.30-29.6  
libdb-4\_8-debuginfo-4.8.30-29.6  
libdb-4\_8-debugsource-4.8.30-29.6  
db48-utils-4.8.30-29.6  
libdb-4\_8-4.8.30-29.6  
libdb-4\_8-debuginfo-32bit-4.8.30-29.6

## 146437 - SuSE SLED 12 SP3 SUSE-SU-2018:0509-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10810

### Description

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

SUSE-SU-2018:0509-1

### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003747.html>

SuSE SLED 12 SP3

x86\_64  
drm-kmp-default-4.9.33\_k4.4.114\_94.11-4.11.1  
drm-kmp-default-debuginfo-4.9.33\_k4.4.114\_94.11-4.11.1

## 146440 - SuSE Linux 42.3 openSUSE-SU-2018:0544-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-9100, CVE-2015-9101, CVE-2017-11720, CVE-2017-13712, CVE-2017-15019, CVE-2017-9410, CVE-2017-9411, CVE-2017-9412, CVE-2017-9869, CVE-2017-9870, CVE-2017-9871, CVE-2017-9872

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0544-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00108.html>

SuSE Linux 42.3

x86\_64

lame-mp3rtp-3.100-7.1

libmp3lame-devel-3.100-7.1

lame-mp3rtp-debuginfo-3.100-7.1

libmp3lame0-3.100-7.1

libmp3lame0-32bit-3.100-7.1

libmp3lame0-debuginfo-32bit-3.100-7.1

lame-debugsource-3.100-7.1

lame-3.100-7.1

libmp3lame0-debuginfo-3.100-7.1

lame-debuginfo-3.100-7.1

lame-doc-3.100-7.1

i586

lame-mp3rtp-3.100-7.1

libmp3lame-devel-3.100-7.1

lame-mp3rtp-debuginfo-3.100-7.1

libmp3lame0-3.100-7.1

lame-debugsource-3.100-7.1

lame-3.100-7.1

libmp3lame0-debuginfo-3.100-7.1

lame-debuginfo-3.100-7.1

lame-doc-3.100-7.1

146441 - SuSE Linux 42.3 openSUSE-SU-2018:0519-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0519-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00090.html>

SuSE Linux 42.3

i586  
libdb-4\_5-4.5.20-135.3.1  
libdb-4\_5-devel-4.5.20-135.3.1  
libdb\_java-4\_5-debuginfo-4.5.20-135.3.1  
libdb-4\_5-debugsource-4.5.20-135.3.1  
db45-utils-4.5.20-135.3.1  
libdb\_java-4\_5-debugsource-4.5.20-135.3.1  
libdb\_java-4\_5-devel-4.5.20-135.3.1  
libdb-4\_5-debuginfo-4.5.20-135.3.1  
libdb\_java-4\_5-4.5.20-135.3.1

noarch  
db45-utils-doc-4.5.20-135.3.1  
db45-doc-4.5.20-135.3.1

x86\_64  
libdb-4\_5-4.5.20-135.3.1  
libdb-4\_5-devel-32bit-4.5.20-135.3.1  
libdb-4\_5-devel-4.5.20-135.3.1  
libdb-4\_5-32bit-4.5.20-135.3.1  
libdb\_java-4\_5-debuginfo-4.5.20-135.3.1  
libdb-4\_5-debugsource-4.5.20-135.3.1  
libdb-4\_5-debuginfo-32bit-4.5.20-135.3.1  
db45-utils-4.5.20-135.3.1  
libdb\_java-4\_5-debugsource-4.5.20-135.3.1  
libdb\_java-4\_5-devel-4.5.20-135.3.1  
libdb-4\_5-debuginfo-4.5.20-135.3.1  
libdb\_java-4\_5-4.5.20-135.3.1

## 163546 - Oracle Enterprise Linux ELSA-2018-4041 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14106, CVE-2017-16525, CVE-2017-16529, CVE-2017-16531, CVE-2017-6951, CVE-2017-7482, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
ELSA-2018-4041

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-February/007539.html>

OEL6  
x86\_64  
kernel-uek-devel-2.6.39-400.298.3.el6uek  
kernel-uek-debug-2.6.39-400.298.3.el6uek  
kernel-uek-firmware-2.6.39-400.298.3.el6uek  
kernel-uek-debug-devel-2.6.39-400.298.3.el6uek  
kernel-uek-2.6.39-400.298.3.el6uek  
kernel-uek-doc-2.6.39-400.298.3.el6uek

i386  
kernel-uek-devel-2.6.39-400.298.3.el6uek  
kernel-uek-debug-2.6.39-400.298.3.el6uek

kernel-uek-firmware-2.6.39-400.298.3.el6uek  
kernel-uek-debug-devel-2.6.39-400.298.3.el6uek  
kernel-uek-2.6.39-400.298.3.el6uek  
kernel-uek-doc-2.6.39-400.298.3.el6uek

## 163547 - Oracle Enterprise Linux ELSA-2018-4040 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14106, CVE-2017-16525, CVE-2017-16526, CVE-2017-16529, CVE-2017-16531, CVE-2017-16535, CVE-2017-7482, CVE-2017-8824, CVE-2017-9074

### Description

The scan detected that the host is missing the following update:  
ELSA-2018-4040

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-February/007538.html>

<http://oss.oracle.com/pipermail/el-errata/2018-February/007537.html>

### OEL7

x86\_64  
kernel-uek-debug-devel-3.8.13-118.20.3.el7uek  
kernel-uek-firmware-3.8.13-118.20.3.el7uek  
kernel-uek-debug-3.8.13-118.20.3.el7uek  
kernel-uek-3.8.13-118.20.3.el7uek  
kernel-uek-doc-3.8.13-118.20.3.el7uek  
kernel-uek-devel-3.8.13-118.20.3.el7uek  
dtrace-modules-3.8.13-118.20.3.el7uek-0.4.5-3.el7

### OEL6

x86\_64  
kernel-uek-3.8.13-118.20.3.el6uek  
kernel-uek-debug-3.8.13-118.20.3.el6uek  
kernel-uek-devel-3.8.13-118.20.3.el6uek  
kernel-uek-doc-3.8.13-118.20.3.el6uek  
kernel-uek-debug-devel-3.8.13-118.20.3.el6uek  
dtrace-modules-3.8.13-118.20.3.el6uek-0.4.5-3.el6  
kernel-uek-firmware-3.8.13-118.20.3.el6uek

## 170930 - Amazon Linux AMI ALAS-2018-957 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5379, CVE-2018-5380, CVE-2018-5381

### Description

The scan detected that the host is missing the following update:  
ALAS-2018-957

### Observation

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



<https://alas.aws.amazon.com/ALAS-2018-957.html>

Amazon Linux AMI

x86\_64

quagga-debuginfo-0.99.22.4-4.17.amzn1

quagga-0.99.22.4-4.17.amzn1

quagga-devel-0.99.22.4-4.17.amzn1

quagga-contrib-0.99.22.4-4.17.amzn1

i686

quagga-debuginfo-0.99.22.4-4.17.amzn1

quagga-0.99.22.4-4.17.amzn1

quagga-devel-0.99.22.4-4.17.amzn1

quagga-contrib-0.99.22.4-4.17.amzn1

## 170931 - Amazon Linux AMI ALAS-2018-954 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3145

### Description

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

ALAS-2018-954

### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2018-954.html>

Amazon Linux AMI

x86\_64

bind-utils-9.8.2-0.62.rc1.57.amzn1

bind-chroot-9.8.2-0.62.rc1.57.amzn1

bind-9.8.2-0.62.rc1.57.amzn1

bind-debuginfo-9.8.2-0.62.rc1.57.amzn1

bind-sdb-9.8.2-0.62.rc1.57.amzn1

bind-libs-9.8.2-0.62.rc1.57.amzn1

bind-devel-9.8.2-0.62.rc1.57.amzn1

i686

bind-utils-9.8.2-0.62.rc1.57.amzn1

bind-chroot-9.8.2-0.62.rc1.57.amzn1

bind-devel-9.8.2-0.62.rc1.57.amzn1

bind-9.8.2-0.62.rc1.57.amzn1

bind-libs-9.8.2-0.62.rc1.57.amzn1

bind-sdb-9.8.2-0.62.rc1.57.amzn1

bind-debuginfo-9.8.2-0.62.rc1.57.amzn1

## 170932 - Amazon Linux AMI ALAS-2018-955 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15134

### Description

The scan detected that the host is missing the following update:  
ALAS-2018-955

### Observation

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

<https://alas.aws.amazon.com/ALAS-2018-955.html>

#### Amazon Linux AMI

##### x86\_64

389-ds-base-devel-1.3.6.1-26.52.amzn1

389-ds-base-1.3.6.1-26.52.amzn1

389-ds-base-snmp-1.3.6.1-26.52.amzn1

389-ds-base-libs-1.3.6.1-26.52.amzn1

389-ds-base-debuginfo-1.3.6.1-26.52.amzn1

##### i686

389-ds-base-devel-1.3.6.1-26.52.amzn1

389-ds-base-1.3.6.1-26.52.amzn1

389-ds-base-snmp-1.3.6.1-26.52.amzn1

389-ds-base-libs-1.3.6.1-26.52.amzn1

389-ds-base-debuginfo-1.3.6.1-26.52.amzn1

## 186109 - Ubuntu Linux 16.04 USN-3582-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8952, CVE-2017-12190, CVE-2017-15115, CVE-2017-17712, CVE-2017-5715, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
USN-3582-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004290.html>

#### Ubuntu 16.04

linux-image-powerpc-smp\_4.4.0.116.122

linux-image-raspi2\_4.4.0.1085.85

linux-image-4.4.0-116-generic\_4.4.0-116.140

linux-image-kvm\_4.4.0.1019.18

linux-image-4.4.0-116-lowlatency\_4.4.0-116.140

linux-image-4.4.0-116-powerpc-smp\_4.4.0-116.140

linux-image-generic\_4.4.0.116.122

linux-image-4.4.0-1087-snapdragon\_4.4.0-1087.92

linux-image-powerpc64-emb\_4.4.0.116.122

linux-image-4.4.0-116-powerpc64-smp\_4.4.0-116.140

linux-image-4.4.0-1019-kvm\_4.4.0-1019.24

linux-image-4.4.0-116-powerpc-e500mc\_4.4.0-116.140

linux-image-lowlatency\_4.4.0.116.122

linux-image-generic-lpae\_4.4.0.116.122

linux-image-4.4.0-116-powerpc64-emb\_4.4.0-116.140  
linux-image-powerpc64-smp\_4.4.0.116.122  
linux-image-4.4.0-1052-aws\_4.4.0-1052.61  
linux-image-powerpc-e500mc\_4.4.0.116.122  
linux-image-4.4.0-116-generic-lpae\_4.4.0-116.140  
linux-image-4.4.0-1085-raspi2\_4.4.0-1085.93  
linux-image-snapdragon\_4.4.0.1087.79  
linux-image-aws\_4.4.0.1052.54

## 186113 - Ubuntu Linux 17.10 USN-3581-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15115, CVE-2017-17712, CVE-2017-5715, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
USN-3581-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004289.html>

Ubuntu 17.10

linux-image-lowlatency\_4.13.0.36.38  
linux-image-generic\_4.13.0.36.38  
linux-image-4.13.0-36-lowlatency\_4.13.0-36.40  
linux-image-4.13.0-36-generic-lpae\_4.13.0-36.40  
linux-image-4.13.0-36-generic\_4.13.0-36.40  
linux-image-generic-lpae\_4.13.0.36.38

## 186114 - Ubuntu Linux 14.04 USN-3582-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8952, CVE-2017-12190, CVE-2017-15115, CVE-2017-17712, CVE-2017-5715, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
USN-3582-2

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004292.html>

Ubuntu 14.04

linux-image-4.4.0-116-lowlatency\_4.4.0-116.140~14.04.1  
linux-image-powerpc-e500mc-lts-xenial\_4.4.0.116.98  
linux-image-powerpc64-emb-lts-xenial\_4.4.0.116.98  
linux-image-powerpc-smp-lts-xenial\_4.4.0.116.98

linux-image-generic-lts-xenial\_4.4.0.116.98  
linux-image-4.4.0-116-generic\_4.4.0-116.140~14.04.1  
linux-image-aws\_4.4.0.1014.14  
linux-image-4.4.0-116-generic-lpae\_4.4.0-116.140~14.04.1  
linux-image-4.4.0-116-powerpc-e500mc\_4.4.0-116.140~14.04.1  
linux-image-4.4.0-1014-aws\_4.4.0-1014.14  
linux-image-4.4.0-116-powerpc64-emb\_4.4.0-116.140~14.04.1  
linux-image-4.4.0-116-powerpc-smp\_4.4.0-116.140~14.04.1  
linux-image-generic-lts-xenial\_4.4.0.116.98  
linux-image-4.4.0-116-powerpc64-smp\_4.4.0-116.140~14.04.1  
linux-image-lowlatency-lts-xenial\_4.4.0.116.98  
linux-image-powerpc64-smp-lts-xenial\_4.4.0.116.98

## 186115 - Ubuntu Linux 17.10 USN-3581-3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15115, CVE-2017-17712, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
USN-3581-3

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004294.html>

Ubuntu 17.10

linux-image-raspi2\_4.13.0.1014.12  
linux-image-4.13.0-1014-raspi2\_4.13.0-1014.15

## 186119 - Ubuntu Linux 16.04 USN-3581-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15115, CVE-2017-17712, CVE-2017-5715, CVE-2017-8824

### Description

The scan detected that the host is missing the following update:  
USN-3581-2

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004291.html>

Ubuntu 16.04

linux-image-oem\_4.13.0.1021.25  
linux-image-gke\_4.13.0.1011.13  
linux-image-4.13.0-36-lowlatency\_4.13.0-36.40~16.04.1  
linux-image-4.13.0-36-generic\_4.13.0-36.40~16.04.1

linux-image-gcp\_4.13.0.1011.13  
linux-image-4.13.0-36-generic-lpae\_4.13.0-36.40~16.04.1  
linux-image-generic-lpae-hwe-16.04\_4.13.0.36.55  
linux-image-4.13.0-1011-azure\_4.13.0-1011.14  
linux-image-4.13.0-1021-oem\_4.13.0-1021.23  
linux-image-4.13.0-1011-gcp\_4.13.0-1011.15  
linux-image-lowlatency-hwe-16.04\_4.13.0.36.55  
linux-image-azure\_4.13.0.1011.12  
linux-image-generic-hwe-16.04\_4.13.0.36.55

### 193300 - Fedora Linux 26 FEDORA-2018-cbc52e8812 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-cbc52e8812

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

irssi-1.0.7-1.fc26

### 193306 - Fedora Linux 27 FEDORA-2018-433d2dc3c7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-433d2dc3c7

#### 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/2018/2/?count=200&page=2>

Fedora Core 27

irssi-1.0.7-1.fc27

### 193319 - Fedora Linux 26 FEDORA-2017-3915878e18 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000231, CVE-2017-1000232

### Description

The scan detected that the host is missing the following update:  
FEDORA-2017-3915878e18

### 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/2018/2/?count=200&page=2>

Fedora Core 26

Idns-1.7.0-4.fc26

## 23152 - (HPESBHF0300) HPE Intelligent Management Center Multiple Denial of Service Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-12559, CVE-2017-12560

### Description

Multiple denial of service vulnerabilities are present in some versions of HPE Intelligent Management Center.

### Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

Multiple denial of service vulnerabilities are present in some versions of HPE Intelligent Management Center. The flaws lie in mibFileServlet servlet. Successful exploitation could allow an attacker to cause denial of service condition.

## 23156 - (VMSA-2018-0006) VMware AirWatch Console Cross-Site Request Forgery Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-4951

### Description

A Cross-Site Request Forgery vulnerability is present in some versions of VMware AirWatch.

### Observation

VMware AirWatch is an enterprise solution for managing mobile devices.

A Cross-Site Request Forgery vulnerability is present in some versions of VMware AirWatch. The flaw lies in the App Catalog. Successful exploitation of this vulnerability could allow an attacker to trick any user to install a malicious app in their device.

## 23164 - (K63675293) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-1548

### Description

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

#### Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the NTP component. Successful exploitation could allow attacker to cause a denial of service condition on the target system.

### 23169 - Apache Tomcat Multiple Vulnerabilities Prior To 7.0.85

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

#### Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

#### Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws are related with security constraints. Successful exploitation could allow an attacker to make unauthorized modification or bypass security access restrictions in the target system.

### 141872 - Red Hat Enterprise Linux RHSA-2018-0350 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

#### Description

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

RHSA-2018-0350

#### Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-February/msg00023.html>

#### RHEL7D

x86\_64

gcab-debuginfo-0.7-4.el7\_4

libgcab1-devel-0.7-4.el7\_4

gcab-0.7-4.el7\_4

libgcab1-0.7-4.el7\_4

#### RHEL7S

x86\_64

gcab-debuginfo-0.7-4.el7\_4

libgcab1-devel-0.7-4.el7\_4

gcab-0.7-4.el7\_4

libgcab1-0.7-4.el7\_4

#### RHEL7WS

x86\_64

gcab-debuginfo-0.7-4.el7\_4  
libgcab1-devel-0.7-4.el7\_4  
gcab-0.7-4.el7\_4  
libgcab1-0.7-4.el7\_4

## 141874 - Red Hat Enterprise Linux RHSA-2018-0352 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

### Description

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

RHSA-2018-0352

### Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2018-February/msg00025.html>

### RHEL6D

x86\_64

java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9

i386

java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9

### RHEL6S

i386

java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9

x86\_64

java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9

### RHEL6WS



x86\_64  
java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9

i386  
java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el6\_9  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el6\_9

## 141876 - Red Hat Enterprise Linux RHSA-2018-0351 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

### Description

The scan detected that the host is missing the following update:  
RHSA-2018-0351

### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-February/msg00024.html>

### RHEL7D

x86\_64  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el7

### RHEL7S

x86\_64  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el7

### RHEL7WS

x86\_64  
java-1.8.0-ibm-devel-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-demo-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-src-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-jdbc-1.8.0.5.10-1jpp.1.el7

java-1.8.0-ibm-1.8.0.5.10-1jpp.1.el7  
java-1.8.0-ibm-plugin-1.8.0.5.10-1jpp.1.el7

### 146438 - SuSE Linux 42.3 openSUSE-SU-2018:0536-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000499, CVE-2018-7260

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0536-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00100.html>

SuSE Linux 42.3  
noarch  
phpMyAdmin-4.7.8-9.1

### 163549 - Oracle Enterprise Linux ELSA-2018-0350 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

#### Description

The scan detected that the host is missing the following update:  
ELSA-2018-0350

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2018-February/007534.html>

OEL7  
x86\_64  
libgcb1-devel-0.7-4.el7\_4  
gcb-0.7-4.el7\_4  
libgcb1-0.7-4.el7\_4

### 170929 - Amazon Linux AMI ALAS-2018-956 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000405, CVE-2017-17741, CVE-2017-5753, CVE-2018-1000028, CVE-2018-5344, CVE-2018-5750

#### Description

The scan detected that the host is missing the following update:  
ALAS-2018-956

## Observation

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

<https://alas.aws.amazon.com/ALAS-2018-956.html>

### Amazon Linux AMI

i686

kernel-headers-4.9.81-35.56.amzn1  
perf-debuginfo-4.9.81-35.56.amzn1  
kernel-tools-devel-4.9.81-35.56.amzn1  
kernel-debuginfo-4.9.81-35.56.amzn1  
kernel-4.9.81-35.56.amzn1  
kernel-debuginfo-common-i686-4.9.81-35.56.amzn1  
kernel-tools-4.9.81-35.56.amzn1  
perf-4.9.81-35.56.amzn1  
kernel-devel-4.9.81-35.56.amzn1  
kernel-tools-debuginfo-4.9.81-35.56.amzn1

noarch

kernel-doc-4.9.81-35.56.amzn1

x86\_64

kernel-headers-4.9.81-35.56.amzn1  
perf-debuginfo-4.9.81-35.56.amzn1  
kernel-debuginfo-common-x86\_64-4.9.81-35.56.amzn1  
kernel-tools-4.9.81-35.56.amzn1  
kernel-tools-devel-4.9.81-35.56.amzn1  
kernel-debuginfo-4.9.81-35.56.amzn1  
kernel-4.9.81-35.56.amzn1  
perf-4.9.81-35.56.amzn1  
kernel-devel-4.9.81-35.56.amzn1  
kernel-tools-debuginfo-4.9.81-35.56.amzn1

## 170933 - Amazon Linux AMI ALAS-2018-951 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000005, CVE-2018-1000007

## Description

The scan detected that the host is missing the following update:  
ALAS-2018-951

## Observation

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

<https://alas.aws.amazon.com/ALAS-2018-951.html>

### Amazon Linux AMI

x86\_64

libcurl-devel-7.53.1-14.81.amzn1  
libcurl-7.53.1-14.81.amzn1  
curl-7.53.1-14.81.amzn1  
curl-debuginfo-7.53.1-14.81.amzn1

i686  
libcurl-7.53.1-14.81.amzn1  
libcurl-devel-7.53.1-14.81.amzn1  
curl-7.53.1-14.81.amzn1  
curl-debuginfo-7.53.1-14.81.amzn1

### 175325 - Scientific Linux Security ERRATA Important: gcab on SL7.x x86\_64 (1802-8874)

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

Risk Level: Medium

CVE: CVE-2018-5345

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: gcab on SL7.x x86\_64 (1802-8874)

#### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1802&L=scientific-linux-errata&F=&S=&P=8874>

SL7  
x86\_64  
gcab-debuginfo-0.7-4.el7\_4  
libgcab1-devel-0.7-4.el7\_4  
gcab-0.7-4.el7\_4  
libgcab1-0.7-4.el7\_4

### 186118 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3584-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17512

#### Description

The scan detected that the host is missing the following update:  
USN-3584-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004298.html>

Ubuntu 16.04

sensible-utils\_0.0.9ubuntu0.16.04.1

Ubuntu 14.04

sensible-utils\_0.0.9ubuntu0.14.04.1

Ubuntu 17.10

sensible-utils\_0.0.10ubuntu0.1

## 193296 - Fedora Linux 26 FEDORA-2018-e23d2dae46 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15565

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-e23d2dae46

### 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/2018/2/?count=200&page=2>

Fedora Core 26

mingw-poppler-0.52.0-6.fc26

## 193298 - Fedora Linux 26 FEDORA-2018-ccef1ced42 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17784, CVE-2017-17785, CVE-2017-17786, CVE-2017-17787, CVE-2017-17788, CVE-2017-17789

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-ccef1ced42

### 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/2018/2/?count=200&page=2>

Fedora Core 26

gimp-2.8.22-3.fc26

## 193321 - Fedora Linux 27 FEDORA-2018-b152c791cc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12596, CVE-2017-9110, CVE-2017-9111, CVE-2017-9112, CVE-2017-9113, CVE-2017-9114, CVE-2017-9115, CVE-2017-9116

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-b152c791cc

### 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/2018/2/?count=200&page=1>

Fedora Core 27

mingw-OpenEXR-2.2.0-7.fc27

#### 193325 - Fedora Linux 26 FEDORA-2018-f5d2f4ec0d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12596, CVE-2017-9110, CVE-2017-9111, CVE-2017-9112, CVE-2017-9113, CVE-2017-9114, CVE-2017-9115, CVE-2017-9116

#### Description

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

FEDORA-2018-f5d2f4ec0d

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

mingw-OpenEXR-2.2.0-6.fc26

#### 193328 - Fedora Linux 26 FEDORA-2018-c54ced412e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5345

#### Description

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

FEDORA-2018-c54ced412e

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

gcab-1.1-1.fc26

#### 23159 - Schneider Electric Interactive Graphical SCADA System Security Misconfiguration Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-9967

### Description

A vulnerability is present in some versions of Schneider Electric Interactive Graphical SCADA System.

### Observation

Schneider Electric Interactive Graphical SCADA System is a software used for monitoring and controlling industrial processes.

A vulnerability is present in some versions of Schneider Electric Interactive Graphical SCADA System. The flaw lies in the memory protection settings. Successful exploitation could allow a local attacker to cause a denial of service condition or execute arbitrary code.

## 23166 - Apache Tomcat Multiple Vulnerabilities Prior To 9.0.5

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

### Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

### Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws are due to improper handling of security constraints on a URL. Successful exploitation could allow an attacker to bypass security restrictions and gain unauthorized access on the target.

## 23168 - Apache Tomcat Multiple Vulnerabilities Prior To 8.0.50

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

### Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

### Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws are due to improper handling of security constraints on a URL. Successful exploitation could allow an attacker to bypass security restrictions and gain unauthorized access on the target.

## 23172 - (K41613034) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-2519

### Description

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

### Observation

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

A vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in the NTP component. Successful exploitation could allow attacker to cause a denial of service condition on the target system.

## 141875 - Red Hat Enterprise Linux RHSA-2018-0349 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

### Description

The scan detected that the host is missing the following update:  
RHSA-2018-0349

### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2018-February/msg00026.html>

### RHEL7S

noarch  
java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el7\_4

### x86\_64

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-headless-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-accessibility-1.7.0.171-2.6.13.0.el7\_4

### RHEL6S

i386  
java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

### noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el6\_9

### x86\_64

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

### RHEL6WS

x86\_64  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9



i386

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

RHEL7D

x86\_64  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-headless-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-accessibility-1.7.0.171-2.6.13.0.el7\_4

noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el7\_4

RHEL6D

i386  
java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el6\_9

x86\_64

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

RHEL7WS

x86\_64  
java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-headless-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el7\_4  
java-1.7.0-openjdk-accessibility-1.7.0.171-2.6.13.0.el7\_4

noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el7\_4

146425 - SuSE Linux 42.3 openSUSE-SU-2018:0522-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5992

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0522-1

## Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00093.html>

SuSE Linux 42.3

noarch

python3-openpyxl-2.2.4-7.3.1

## 163548 - Oracle Enterprise Linux ELSA-2018-0349 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

## Description

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

ELSA-2018-0349

## Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2018-February/007536.html>

<http://oss.oracle.com/pipermail/el-errata/2018-February/007535.html>

OEL7

x86\_64

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-headless-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-accessibility-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.0.1.el7\_4

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.0.1.el7\_4

OEL6

x86\_64

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.0.1.el6\_9

i386

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.0.1.el6\_9

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.0.1.el6\_9

## 170934 - Amazon Linux AMI ALAS-2018-959 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15706

### Description

The scan detected that the host is missing the following update:  
ALAS-2018-959

### Observation

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

<https://alas.aws.amazon.com/ALAS-2018-959.html>

Amazon Linux AMI

noarch

tomcat8-8.5.28-1.76.amzn1

tomcat8-jsp-2.3-api-8.5.28-1.76.amzn1

tomcat8-webapps-8.5.28-1.76.amzn1

tomcat8-admin-webapps-8.5.28-1.76.amzn1

tomcat8-docs-webapp-8.5.28-1.76.amzn1

tomcat8-servlet-3.1-api-8.5.28-1.76.amzn1

tomcat8-el-3.0-api-8.5.28-1.76.amzn1

tomcat8-javadoc-8.5.28-1.76.amzn1

tomcat8-log4j-8.5.28-1.76.amzn1

tomcat8-lib-8.5.28-1.76.amzn1

175326 - Scientific Linux Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (1802-9195)

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (1802-9195)

### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1802&L=scientific-linux-errata&F=&S=&P=9195>

SL7

x86\_64

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-headless-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el7\_4

java-1.7.0-openjdk-accessibility-1.7.0.171-2.6.13.0.el7\_4

noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el7\_4

SL6

i386

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

noarch

java-1.7.0-openjdk-javadoc-1.7.0.171-2.6.13.0.el6\_9

x86\_64

java-1.7.0-openjdk-src-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-demo-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-devel-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-debuginfo-1.7.0.171-2.6.13.0.el6\_9

java-1.7.0-openjdk-1.7.0.171-2.6.13.0.el6\_9

### 182623 - FreeBSD LibreOffice Remote Arbitrary File Disclosure Vulnerability Via WEBSERVICE Formula (289269f1-0def-11e8-99b0-d017c2987f9a)

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Description

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

LibreOffice -- Remote arbitrary file disclosure vulnerability via WEBSERVICE formula (289269f1-0def-11e8-99b0-d017c2987f9a)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/289269f1-0def-11e8-99b0-d017c2987f9a.html>

Affected packages:

libreoffice < 5.4.5

6.0.0 <= libreoffice < 6.0.1

### 182629 - FreeBSD cvs Remote Code Execution Via Ssh Command Injection (d9fe59ea-1940-11e8-9eb8-5404a68ad561)

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

Risk Level: Medium

CVE: CVE-2017-12836

#### Description

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

cvs -- Remote code execution via ssh command injection (d9fe59ea-1940-11e8-9eb8-5404a68ad561)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/d9fe59ea-1940-11e8-9eb8-5404a68ad561.html>

Affected packages:  
cvs < 1.20120905\_5

### 186116 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3579-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Description

The scan detected that the host is missing the following update:  
USN-3579-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004287.html>

Ubuntu 16.04

libreoffice-core\_5.1.6~rc2-0ubuntu1~xenial3

Ubuntu 14.04

libreoffice-core\_4.2.8-0ubuntu5.3

Ubuntu 17.10

libreoffice-core\_5.4.5-0ubuntu0.17.10.1

### 193320 - Fedora Linux 26 FEDORA-2018-4367d984c1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6644

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-4367d984c1

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

sblim-sfcb-1.4.9-7.fc26

### 193326 - Fedora Linux 27 FEDORA-2018-9d6a122887 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6644

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-9d6a122887

#### 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/2018/2/?count=200&page=1>

Fedora Core 27

sblim-sfcb-1.4.9-9.fc27

### 23153 - (K54358225) F5 BIG-IP BIG-IP APM Portal Access Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-0301

#### Description

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

#### Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in BIG-IP APM logging. Successful exploitation could allow a remote authenticated user to access different internal resources than intended.

### 23174 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.28

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

Risk Level: Medium

CVE: CVE-2018-1304, CVE-2018-1305

#### Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

#### Observation

Apache Tomcat is an open source software implementation of the Java Servlet and Java Server Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws are due to improper handling of security constraints. Successful exploitation could allow an attacker to bypass security restrictions and gain unauthorized access on the target.

### 88918 - Slackware Linux 14.2 SSA:2018-057-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5753

### Description

The scan detected that the host is missing the following update:  
SSA:2018-057-01

### 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=2018&m=slackware-security.684951>

Slackware 14.2

i586

kernel-modules-4.4.118-i586-1

kernel-huge-4.4.118-i586-1

kernel-generic-4.4.118-i586-1

i686

kernel-generic-smp-4.4.118\_smp-i686-1

kernel-huge-smp-4.4.118\_smp-i686-1

kernel-modules-smp-4.4.118\_smp-i686-1

noarch

kernel-source-4.4.118-noarch-1

kernel-firmware-20180222\_7344ec9-noarch-1

kernel-source-4.4.118\_smp-noarch-1

x86\_64

kernel-huge-4.4.118-x86\_64-1

kernel-modules-4.4.118-x86\_64-1

kernel-generic-4.4.118-x86\_64-1

## 131031 - Debian Linux 9.0 DSA-4120-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13166, CVE-2017-5715, CVE-2017-5754, CVE-2018-5750

### Description

The scan detected that the host is missing the following update:  
DSA-4120-1

### Observation

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

<http://www.debian.org/security/2018/dsa-4120>

Debian 9.0

all

scsi-core-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2

loop-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2

linux-headers-4.9.0-4-all-mips\_4.9.82-1+deb9u2

firewire-core-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2

nbd-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2

crypto-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2

usb-storage-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2

jfs-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
affs-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
md-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-all-armhf\_4.9.82-1+deb9u2  
efi-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
md-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
nbd-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
scsi-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
acpi-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
jfs-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
fb-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
sound-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
i2c-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
ppp-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
affs-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
affs-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
ata-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-4kc-malta\_4.9.82-1+deb9u2  
zlib-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
multipath-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
isofs-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
kernel-image-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
crypto-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
pcmcia-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-s390x\_4.9.82-1+deb9u2  
zlib-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
kernel-image-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
fat-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
mmc-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
usb-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
crc-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
input-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
i2c-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
linux-image-4.9.0-4-octeon-dbg\_4.9.82-1+deb9u2  
virtio-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
fuse-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
crc-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
event-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
scsi-core-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
cdrom-core-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-amd64\_4.9.82-1+deb9u2  
sound-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
multipath-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
kernel-image-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
scsi-core-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
scsi-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
sata-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
fuse-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
btrfs-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
linux-image-4.9.0-4-amd64-dbg\_4.9.82-1+deb9u2  
loop-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
minix-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
squashfs-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
nic-pcmcia-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
ppp-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
udf-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
hyperv-daemons\_4.9.82-1+deb9u2



udf-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
multipath-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
fuse-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
dasd-extra-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
event-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
nic-wireless-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
scsi-core-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
hypervisor-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
input-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
nfs-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
kernel-image-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
acpi-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
usb-serial-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
loop-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
btrfs-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
ppp-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
linux-image-4.9.0-4-rt-686-pae-dbg\_4.9.82-1+deb9u2  
udf-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
multipath-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
fuse-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
loop-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
fb-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
isofs-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
pcmcia-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
nic-wireless-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
efi-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
mmc-core-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
linux-image-4.9.0-4-armmp-lpae\_4.9.82-1+deb9u2  
sata-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
event-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
zlib-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
mtd-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
linux-image-4.9.0-4-686-pae-dbg\_4.9.82-1+deb9u2  
ext4-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
event-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
isofs-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
fat-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
i2c-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
kernel-image-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
squashfs-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
scsi-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
crc-modules-4.9.0-4-arm64-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-all-mipsel\_4.9.82-1+deb9u2  
virtio-modules-4.9.0-4-686-pae-di\_4.9.82-1+deb9u2  
uinput-modules-4.9.0-4-marvell-di\_4.9.82-1+deb9u2  
squashfs-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
pcmcia-storage-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
nic-usb-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
nic-shared-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
sata-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
udf-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
input-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
linux-headers-4.9.0-4-marvell\_4.9.82-1+deb9u2  
fat-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
usb-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2  
usb-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
crypto-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
mmc-core-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2

btrfs-modules-4.9.0-4-amd64-di\_4.9.82-1+deb9u2  
nic-modules-4.9.0-4-s390x-di\_4.9.82-1+deb9u2  
isofs-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
mouse-modules-4.9.0-4-4kc-malta-di\_4.9.82-1+deb9u2  
nic-wireless-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
isofs-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
serial-modules-4.9.0-4-powerpc64le-di\_4.9.82-1+deb9u2  
scsi-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
ntfs-modules-4.9.0-4-loongson-3-di\_4.9.82-1+deb9u2  
md-modules-4.9.0-4-686-di\_4.9.82-1+deb9u2  
mmc-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
crc-modules-4.9.0-4-armmp-di\_4.9.82-1+deb9u2  
virtio-modules-4.9.0-4-5kc-malta-di\_4.9.82-1+deb9u2  
multipath-modules-4.9.0-4-octeon-di\_4.9.82-1+deb9u2

146421 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0546-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18078

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2018:0546-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003753.html>

SuSE SLES 12 SP2

noarch

systemd-bash-completion-228-150.32.1

x86\_64

libudev1-debuginfo-228-150.32.1

libudev1-228-150.32.1

libsystemd0-228-150.32.1

libudev1-debuginfo-32bit-228-150.32.1

systemd-228-150.32.1

systemd-debuginfo-228-150.32.1

systemd-32bit-228-150.32.1

udev-debuginfo-228-150.32.1

libsystemd0-debuginfo-228-150.32.1

systemd-debugsource-228-150.32.1

libsystemd0-32bit-228-150.32.1

udev-228-150.32.1

systemd-debuginfo-32bit-228-150.32.1

libudev1-32bit-228-150.32.1

systemd-sysvinit-228-150.32.1

libsystemd0-debuginfo-32bit-228-150.32.1

SuSE SLED 12 SP3

x86\_64

libudev1-debuginfo-32bit-228-150.32.1

libudev1-228-150.32.1

libsystemd0-228-150.32.1

systemd-32bit-228-150.32.1  
systemd-228-150.32.1  
systemd-debuginfo-228-150.32.1  
udev-debuginfo-228-150.32.1  
libsystemd0-debuginfo-228-150.32.1  
systemd-debugsource-228-150.32.1  
libudev1-debuginfo-228-150.32.1  
libsystemd0-32bit-228-150.32.1  
udev-228-150.32.1  
libsystemd0-debuginfo-32bit-228-150.32.1  
libudev1-32bit-228-150.32.1  
systemd-sysvinit-228-150.32.1  
systemd-debuginfo-32bit-228-150.32.1

noarch  
systemd-bash-completion-228-150.32.1

### SuSE SLED 12 SP2

x86\_64  
libudev1-debuginfo-32bit-228-150.32.1  
libudev1-228-150.32.1  
libsystemd0-228-150.32.1  
systemd-32bit-228-150.32.1  
systemd-228-150.32.1  
systemd-debuginfo-228-150.32.1  
udev-debuginfo-228-150.32.1  
libsystemd0-debuginfo-228-150.32.1  
systemd-debugsource-228-150.32.1  
libudev1-debuginfo-228-150.32.1  
libsystemd0-32bit-228-150.32.1  
udev-228-150.32.1  
libsystemd0-debuginfo-32bit-228-150.32.1  
libudev1-32bit-228-150.32.1  
systemd-sysvinit-228-150.32.1  
systemd-debuginfo-32bit-228-150.32.1

noarch  
systemd-bash-completion-228-150.32.1

### SuSE SLES 12 SP3

noarch  
systemd-bash-completion-228-150.32.1

x86\_64  
libudev1-debuginfo-228-150.32.1  
libudev1-228-150.32.1  
libsystemd0-228-150.32.1  
libudev1-debuginfo-32bit-228-150.32.1  
systemd-228-150.32.1  
systemd-debuginfo-228-150.32.1  
systemd-32bit-228-150.32.1  
udev-debuginfo-228-150.32.1  
libsystemd0-debuginfo-228-150.32.1  
systemd-debugsource-228-150.32.1  
libsystemd0-32bit-228-150.32.1  
udev-228-150.32.1  
systemd-debuginfo-32bit-228-150.32.1  
libudev1-32bit-228-150.32.1  
systemd-sysvinit-228-150.32.1  
libsystemd0-debuginfo-32bit-228-150.32.1

## 146428 - SuSE Linux 42.3 openSUSE-SU-2018:0561-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6381, CVE-2018-6484, CVE-2018-6540

### Description

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

openSUSE-SU-2018:0561-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00110.html>

SuSE Linux 42.3

x86\_64

libzip-0-13-debuginfo-0.13.67-13.3.1

libzip-0-13-32bit-0.13.67-13.3.1

zzip-devel-32bit-0.13.67-13.3.1

libzip-0-13-0.13.67-13.3.1

zzip-debugsource-0.13.67-13.3.1

zzip-devel-0.13.67-13.3.1

libzip-0-13-debuginfo-32bit-0.13.67-13.3.1

zzip-devel-debuginfo-32bit-0.13.67-13.3.1

zzip-devel-debuginfo-0.13.67-13.3.1

i586

libzip-0-13-debuginfo-0.13.67-13.3.1

zzip-debugsource-0.13.67-13.3.1

libzip-0-13-0.13.67-13.3.1

zzip-devel-0.13.67-13.3.1

zzip-devel-debuginfo-0.13.67-13.3.1

## 146429 - SuSE Linux 42.3 openSUSE-SU-2018:0560-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18078

### Description

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

openSUSE-SU-2018:0560-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00109.html>

SuSE Linux 42.3

i586

nss-myhostname-debuginfo-228-44.1

systemd-mini-228-44.1

libudev1-228-44.1

libsystemd0-debuginfo-228-44.1  
libudev1-debuginfo-228-44.1  
udev-mini-debuginfo-228-44.1  
libudev-mini-devel-228-44.1  
libsystemd0-mini-debuginfo-228-44.1  
systemd-mini-debugsource-228-44.1  
systemd-mini-debuginfo-228-44.1  
systemd-mini-devel-228-44.1  
systemd-debugsource-228-44.1  
udev-228-44.1  
libudev-devel-228-44.1  
libudev-mini1-debuginfo-228-44.1  
systemd-228-44.1  
nss-myhostname-228-44.1  
nss-mymachines-228-44.1  
systemd-debuginfo-228-44.1  
nss-mymachines-debuginfo-228-44.1  
libudev-mini1-228-44.1  
systemd-sysvinit-228-44.1  
udev-mini-228-44.1  
systemd-mini-sysvinit-228-44.1  
udev-debuginfo-228-44.1  
libsystemd0-228-44.1  
systemd-devel-228-44.1  
systemd-logger-228-44.1  
libsystemd0-mini-228-44.1

noarch

systemd-bash-completion-228-44.1  
systemd-mini-bash-completion-228-44.1

x86\_64

nss-myhostname-debuginfo-228-44.1  
nss-myhostname-32bit-228-44.1  
libsystemd0-debuginfo-32bit-228-44.1  
systemd-mini-228-44.1  
libudev1-228-44.1  
libudev1-32bit-228-44.1  
libsystemd0-debuginfo-228-44.1  
nss-myhostname-debuginfo-32bit-228-44.1  
libudev1-debuginfo-228-44.1  
udev-mini-debuginfo-228-44.1  
libudev-mini-devel-228-44.1  
libsystemd0-mini-debuginfo-228-44.1  
systemd-debuginfo-32bit-228-44.1  
systemd-mini-debugsource-228-44.1  
libsystemd0-32bit-228-44.1  
systemd-mini-debuginfo-228-44.1  
systemd-mini-devel-228-44.1  
systemd-debugsource-228-44.1  
udev-228-44.1  
libudev-devel-228-44.1  
libudev-mini1-debuginfo-228-44.1  
systemd-228-44.1  
nss-myhostname-228-44.1  
nss-mymachines-228-44.1  
systemd-debuginfo-228-44.1  
nss-mymachines-debuginfo-228-44.1  
libudev1-debuginfo-32bit-228-44.1  
systemd-32bit-228-44.1

libudev-mini1-228-44.1  
systemd-sysvinit-228-44.1  
udev-mini-228-44.1  
systemd-mini-sysvinit-228-44.1  
udev-debuginfo-228-44.1  
libsystemd0-228-44.1  
systemd-devel-228-44.1  
systemd-logger-228-44.1  
libsystemd0-mini-228-44.1

#### 146431 - SuSE Linux 42.3 openSUSE-SU-2018:0535-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11546, CVE-2017-11547

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0535-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00099.html>

SuSE Linux 42.3  
x86\_64  
timidity-debuginfo-2.14.0-9.3.1  
timidity-2.14.0-9.3.1  
timidity-debugsource-2.14.0-9.3.1

i586  
timidity-debuginfo-2.14.0-9.3.1  
timidity-2.14.0-9.3.1  
timidity-debugsource-2.14.0-9.3.1

#### 146434 - SuSE Linux 42.3 openSUSE-SU-2018:0528-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-8374

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2018:0528-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2018-02/msg00096.html>

SuSE Linux 42.3  
x86\_64  
libmad0-0.15.1b-5.1

libmad-devel-0.15.1b-5.1  
libmad-debugsource-0.15.1b-5.1  
libmad0-debuginfo-0.15.1b-5.1  
libmad0-32bit-0.15.1b-5.1  
libmad0-debuginfo-32bit-0.15.1b-5.1

i586  
libmad0-0.15.1b-5.1  
libmad-debugsource-0.15.1b-5.1  
libmad-devel-0.15.1b-5.1  
libmad0-debuginfo-0.15.1b-5.1

## 146439 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2018:0548-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6381, CVE-2018-6484, CVE-2018-6540

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2018:0548-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2018-February/003754.html>

SuSE SLED 12 SP3  
x86\_64  
libzip-0-13-debuginfo-0.13.67-10.5.1  
libzip-0-13-0.13.67-10.5.1  
zip-devel-0.13.67-10.5.1

SuSE SLED 12 SP2  
x86\_64  
libzip-0-13-debuginfo-0.13.67-10.5.1  
libzip-0-13-0.13.67-10.5.1  
zip-devel-0.13.67-10.5.1

## 182625 - FreeBSD ntp Multiple Vulnerabilities (af485ef4-1c58-11e8-8477-d05099c0ae8c)

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

Risk Level: Medium

CVE: CVE-2016-1549, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185

### Description

The scan detected that the host is missing the following update:  
ntp -- multiple vulnerabilities (af485ef4-1c58-11e8-8477-d05099c0ae8c)

### Observation

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

<http://www.vuxml.org/freebsd/af485ef4-1c58-11e8-8477-d05099c0ae8c.html>

Affected packages:

11.1 <= FreeBSD < 11.1\_7

10.4 <= FreeBSD < 10.4\_6

10.3 <= FreeBSD < 10.3\_27

ntp < 4.2.8p11

## 186110 - Ubuntu Linux 12.04 USN-3580-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753

### Description

The scan detected that the host is missing the following update:  
USN-3580-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-February/004288.html>

Ubuntu 12.04

linux-image-generic-pae\_3.2.0.133.148

linux-image-3.2.0-133-generic\_3.2.0-133.179

linux-image-3.2.0-133-generic-pae\_3.2.0-133.179

linux-image-generic\_3.2.0.133.148

## 193301 - Fedora Linux 27 FEDORA-2018-fe5a6ed3b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000002

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-fe5a6ed3b7

### 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/2018/2/?count=200&page=1>

Fedora Core 27

knot-resolver-2.1.0-1.fc27

## 193308 - Fedora Linux 26 FEDORA-2018-844a1e9778 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000002



### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-844a1e9778

### 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/2018/2/?count=200&page=2>

Fedora Core 26

knot-resolver-2.1.0-1.fc26

## 193312 - Fedora Linux 27 FEDORA-2018-418e67c843 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7697

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-418e67c843

### 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/2018/2/?count=200&page=1>

Fedora Core 27

libsamplerate-0.1.9-1.fc27

## 193327 - Fedora Linux 27 FEDORA-2018-da6f76b446 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000051, CVE-2018-6187, CVE-2018-6192, CVE-2018-6544

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-da6f76b446

### 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/2018/2/?count=200&page=2>

Fedora Core 27

mupdf-1.12.0-5.fc27

## 131029 - Debian Linux 8.0, 9.0 DSA-4123-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6932

### Description

The scan detected that the host is missing the following update:  
DSA-4123-1

### Observation

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

<http://www.debian.org/security/2018/dsa-4123>

Debian 8.0  
all  
drupal7\_7.32-1+deb8u10

Debian 9.0  
all  
drupal7\_7.52-2+deb9u2

## 131030 - Debian Linux 8.0, 9.0 DSA-4126-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0489

### Description

The scan detected that the host is missing the following update:  
DSA-4126-1

### Observation

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

<http://www.debian.org/security/2018/dsa-4126>

Debian 8.0  
all  
xmltooling-schemas\_1.5.3-2+deb8u3  
libxmltooling-dev\_1.5.3-2+deb8u3  
libxmltooling6\_1.5.3-2+deb8u3  
libxmltooling-doc\_1.5.3-2+deb8u3

Debian 9.0  
all  
libxmltooling7\_1.6.0-4+deb9u1  
libxmltooling-doc\_1.6.0-4+deb9u1  
xmltooling-schemas\_1.6.0-4+deb9u1  
libxmltooling-dev\_1.6.0-4+deb9u1

## 131032 - Debian Linux 8.0, 9.0 DSA-4122-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-100024, CVE-2018-100027

#### Description

The scan detected that the host is missing the following update:  
DSA-4122-1

#### Observation

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

<http://www.debian.org/security/2018/dsa-4122>

Debian 8.0  
all  
squid3\_3.4.8-6+deb8u5

Debian 9.0  
all  
squid3\_3.5.23-5+deb9u1

### 131033 - Debian Linux 9.0 DSA-4121-1 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-4121-1

#### Observation

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

<http://www.debian.org/security/2018/dsa-4121>

Debian 9.0  
all  
gcc-6\_6.3.0-18+deb9u1

### 182620 - FreeBSD asterisk Multiple Vulnerabilities (933654ce-17b8-11e8-90b8-001999f8d30b)

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

Risk Level: Low

CVE: CVE-2018-7284, CVE-2018-7286

#### Description

The scan detected that the host is missing the following update:  
asterisk -- multiple vulnerabilities (933654ce-17b8-11e8-90b8-001999f8d30b)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/933654ce-17b8-11e8-90b8-001999f8d30b.html>

Affected packages:

asterisk13 < 13.19.2

### 182621 - FreeBSD drupal Drupal Core - Multiple Vulnerabilities (57580fcc-1a61-11e8-97e0-00e04c1ea73d)

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

Risk Level: Low

CVE: CVE-2017-6926, CVE-2017-6927, CVE-2017-6928, CVE-2017-6929, CVE-2017-6930, CVE-2017-6931, CVE-2017-6932

#### Description

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

drupal -- Drupal Core - Multiple Vulnerabilities (57580fcc-1a61-11e8-97e0-00e04c1ea73d)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/57580fcc-1a61-11e8-97e0-00e04c1ea73d.html>

Affected packages:

drupal7 < 7.56

drupal8 < 8.4.4

### 182622 - FreeBSD tomcat Security Constraints Ignored Or Applied Too Late (55c4233e-1844-11e8-a712-0025908740c2)

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

Risk Level: Low

CVE: CVE-2018-1304, CVE-2018-1305

#### Description

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

tomcat -- Security constraints ignored or applied too late (55c4233e-1844-11e8-a712-0025908740c2)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/55c4233e-1844-11e8-a712-0025908740c2.html>

Affected packages:

7.0.0 <= tomcat <= 7.0.84

8.0.0 <= tomcat <= 8.0.49

8.5.0 <= tomcat <= 8.5.27

9.0.0 <= tomcat <= 9.0.4

### 182624 - FreeBSD chromium Vulnerability (abfc932e-1ba8-11e8-a944-54ee754af08e)

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

Risk Level: Low

CVE: CVE-2018-6056

### Description

The scan detected that the host is missing the following update:  
chromium -- vulnerability (abfc932e-1ba8-11e8-a944-54ee754af08e)

### Observation

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

<http://www.vuxml.org/freebsd/abfc932e-1ba8-11e8-a944-54ee754af08e.html>

Affected packages:

chromium < 64.0.3282.167

182626 - FreeBSD asterisk and pjsip Multiple Vulnerabilities (f9f5c5a2-17b5-11e8-90b8-001999f8d30b)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
asterisk and pjsip -- multiple vulnerabilities (f9f5c5a2-17b5-11e8-90b8-001999f8d30b)

### Observation

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

<http://www.vuxml.org/freebsd/f9f5c5a2-17b5-11e8-90b8-001999f8d30b.html>

Affected packages:

asterisk13 < 13.19.2

pjsip < 2.7.2

pjsip-extsrtp < 2.7.2

182627 - FreeBSD chromium Multiple Vulnerabilities (8e986b2b-1baa-11e8-a944-54ee754af08e)

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

Risk Level: Low

CVE: CVE-2017-15420, CVE-2018-6031, CVE-2018-6032, CVE-2018-6033, CVE-2018-6034, CVE-2018-6035, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6039, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6043, CVE-2018-6045, CVE-2018-6046, CVE-2018-6047, CVE-2018-6048, CVE-2018-6049, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

### Description

The scan detected that the host is missing the following update:  
chromium -- multiple vulnerabilities (8e986b2b-1baa-11e8-a944-54ee754af08e)

### Observation

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

<http://www.vuxml.org/freebsd/8e986b2b-1baa-11e8-a944-54ee754af08e.html>

Affected packages:

chromium < 64.0.3282.119

182628 - FreeBSD shibboleth-sp Vulnerable To Forged User Attribute Data (22438240-1bd0-11e8-a2ec-6cc21735f730)

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

Risk Level: Low

CVE: CVE-2018-0489

#### Description

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

shibboleth-sp -- vulnerable to forged user attribute data (22438240-1bd0-11e8-a2ec-6cc21735f730)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/22438240-1bd0-11e8-a2ec-6cc21735f730.html>

Affected packages:

xmltooling < 1.6.4

xerces-c3 < 3.1.4

182630 - FreeBSD phpMyAdmin Self XSS In Central Columns Feature (261ca31c-179f-11e8-b8b9-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2018-7260

#### Description

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

phpMyAdmin -- self XSS in central columns feature (261ca31c-179f-11e8-b8b9-6805ca0b3d42)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/261ca31c-179f-11e8-b8b9-6805ca0b3d42.html>

Affected packages:

4.7.0 <= phpMyAdmin < 4.7.8

182631 - FreeBSD squid Vulnerable To Denial Of Service Attack (d5b6d151-1887-11e8-94f7-9c5c8e75236a)

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

Risk Level: Low

CVE: CVE-2018-100024, CVE-2018-100027

#### Description

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

squid -- Vulnerable to Denial of Service attack (d5b6d151-1887-11e8-94f7-9c5c8e75236a)

### Observation

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

<http://www.vuxml.org/freebsd/d5b6d151-1887-11e8-94f7-9c5c8e75236a.html>

Affected packages:  
squid < 3.5.27\_3  
squid-devel < 4.0.23

### 193297 - Fedora Linux 26 FEDORA-2018-6f08b79a09 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-2018-6574

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-6f08b79a09

### 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/2018/2/?count=200&page=2>

Fedora Core 26

golang-1.8.7-1.fc26

### 193299 - Fedora Linux 27 FEDORA-2018-a1650ed14f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-2018-7260

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-a1650ed14f

### 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/2018/2/?count=200&page=2>

Fedora Core 27

phpMyAdmin-4.7.8-1.fc27  
php-phpmyadmin-sql-parser-4.2.4-3.fc27  
php-phpmyadmin-motranslator-4.0-1.fc27

### 193302 - Fedora Linux 27 FEDORA-2018-7a62047e30 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000026

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-7a62047e30

#### 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/2018/2/?count=200&page=2>

Fedora Core 27

kernel-4.15.4-300.fc27

### 193303 - Fedora Linux 26 FEDORA-2018-c0d3db441f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15407, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15415, CVE-2017-15416, CVE-2017-15418, CVE-2017-15419, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2018-6031, CVE-2018-6033, CVE-2018-6034, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6047, CVE-2018-6048, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-2018-6054

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-c0d3db441f

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

qt5-qtwebengine-5.10.1-1.fc26

### 193304 - Fedora Linux 26 FEDORA-2018-03a6606cb5 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000026

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-03a6606cb5

#### 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/2018/2/?count=200&page=2>

Fedora Core 26

kernel-4.15.4-200.fc26

#### 193305 - Fedora Linux 27 FEDORA-2018-cb1f26bd2c 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-2018-cb1f26bd2c

##### 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/2018/2/?count=200&page=1>

Fedora Core 27

unbound-1.6.8-6.fc27

#### 193307 - Fedora Linux 27 FEDORA-2018-c6cb18d057 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-2018-c6cb18d057

##### 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/2018/2/?count=200&page=2>

Fedora Core 27

seamoney-2.49.2-2.fc27

#### 193309 - Fedora Linux 27 FEDORA-2018-e08d828ed9 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15407, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15415, CVE-2017-15416, CVE-2017-15418, CVE-2017-15419, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2018-6031, CVE-2018-6033, CVE-2018-6034, CVE-2018-6036, CVE-2018-6037, CVE-2018-6038, CVE-2018-6040, CVE-2018-6041, CVE-2018-6042, CVE-2018-6047, CVE-2018-6048, CVE-2018-6050, CVE-2018-6051, CVE-2018-6052, CVE-2018-6053, CVE-

2018-6054

Description

The scan detected that the host is missing the following update:  
FEDORA-2018-e08d828ed9

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/2018/2/?count=200&page=2>

Fedora Core 27

qt5-qtwebengine-5.10.1-1.fc27

193310 - Fedora Linux 27 FEDORA-2018-913c225b49 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6594

Description

The scan detected that the host is missing the following update:  
FEDORA-2018-913c225b49

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/2018/2/?count=200&page=1>

Fedora Core 27

python-crypto-2.6.1-22.fc27

193311 - Fedora Linux 26 FEDORA-2018-b3de6c389e 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-2018-b3de6c389e

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/2018/2/?count=200&page=3>

Fedora Core 26

torbrowser-launcher-0.2.9-1.fc26

## 193313 - Fedora Linux 26 FEDORA-2018-7d90e269a4 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-2018-7d90e269a4

### 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/2018/2/?count=200&page=2>

Fedora Core 26

milkytracker-1.01.00-1.fc26

## 193314 - Fedora Linux 26 FEDORA-2018-25a7ba3cb6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6789

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-25a7ba3cb6

### 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/2018/2/?count=200&page=2>

Fedora Core 26

exim-4.90.1-2.fc26

## 193315 - Fedora Linux 27 FEDORA-2018-2f1f243787 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-2018-2f1f243787

### 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/2018/2/?count=200&page=1>

Fedora Core 27

dnsmasq-2.78-5.fc27

#### 193316 - Fedora Linux 27 FEDORA-2018-eea8cb8b0e 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-2018-eea8cb8b0e

##### 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/2018/2/?count=200&page=1>

Fedora Core 27

systemd-234-10.git5f8984e.fc27

#### 193317 - Fedora Linux 26 FEDORA-2018-b2d76ba048 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-2018-b2d76ba048

##### 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/2018/2/?count=200&page=2>

Fedora Core 26

seamonkey-2.49.2-2.fc26

#### 193318 - Fedora Linux 27 FEDORA-2018-ee417c4b28 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6794

---

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-ee417c4b28

### 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/2018/2/?count=200&page=2>

Fedora Core 27

suricata-4.0.4-1.fc27

## 193322 - Fedora Linux 27 FEDORA-2018-5aec14e125 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6789

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-5aec14e125

### 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/2018/2/?count=200&page=2>

Fedora Core 27

exim-4.90.1-2.fc27

## 193323 - Fedora Linux 27 FEDORA-2018-3ba1be2e79 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-6767, CVE-2018-7253

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-3ba1be2e79

### 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/2018/2/?count=200&page=1>

Fedora Core 27

wavpack-5.1.0-7.fc27

## 193324 - Fedora Linux 27 FEDORA-2018-2331a462fb 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-2018-2331a462fb

### 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/2018/2/?count=200&page=2>

Fedora Core 27

milkytracker-1.01.00-1.fc27

## 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.

### 22778 - (HPESBHF03768) HPE Intelligent Management Center Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-12487, CVE-2017-12488, CVE-2017-12489, CVE-2017-12490, CVE-2017-12491, CVE-2017-12492, CVE-2017-12493, CVE-2017-12494, CVE-2017-12495, CVE-2017-12496, CVE-2017-12497, CVE-2017-12498, CVE-2017-12499, CVE-2017-12500, CVE-2017-12501, CVE-2017-12502, CVE-2017-12503, CVE-2017-12504, CVE-2017-12505, CVE-2017-12506, CVE-2017-12507, CVE-2017-12508, CVE-2017-12509, CVE-2017-12510, CVE-2017-12511, CVE-2017-12512, CVE-2017-12513, CVE-2017-12514, CVE-2017-12515, CVE-2017-12516, CVE-2017-12517, CVE-2017-12518, CVE-2017-12519, CVE-2017-12520, CVE-2017-12521, CVE-2017-12522, CVE-2017-12523, CVE-2017-12524, CVE-2017-12525, CVE-2017-12526, CVE-2017-12527, CVE-2017-12528, CVE-2017-12529, CVE-2017-12530, CVE-2017-12531, CVE-2017-12532, CVE-2017-12533, CVE-2017-12534, CVE-2017-12535, CVE-2017-12536, CVE-2017-12537, CVE-2017-12538, CVE-2017-12539, CVE-2017-12540, CVE-2017-12541

### Update Details

Risk is updated

### 22804 - (HPESBHF03787) HPE Intelligent Management Center Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-8962, CVE-2017-8963, CVE-2017-8964, CVE-2017-8965, CVE-2017-8966, CVE-2017-8967

### Update Details

Risk is updated

### 88917 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-046-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

[Update Details](#)

Risk is updated

### 130913 - Debian Linux 8.0, 9.0 DSA-4004-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7525

[Update Details](#)

Risk is updated

### 182614 - FreeBSD irssi Multiple Vulnerabilities (7afc5e56-156d-11e8-95f2-005056925db4)

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

Risk Level: High

CVE: CVE-2018-7050, CVE-2018-7051, CVE-2018-7052, CVE-2018-7053, CVE-2018-7054

[Update Details](#)

Risk is updated

### 192466 - Fedora Linux 24 FEDORA-2017-8df9efed5f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7525

[Update Details](#)

Risk is updated

### 192503 - Fedora Linux 26 FEDORA-2017-6a75c816fa Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7525

[Update Details](#)

Risk is updated

### 192518 - Fedora Linux 25 FEDORA-2017-f452765e1e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7525

[Update Details](#)

Risk is updated

---

## 192922 - Fedora Linux 27 FEDORA-2017-4a071ecbc7 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-7525

### Update Details

Risk is updated

## 192975 - Fedora Linux 26 FEDORA-2017-e16ed3f7a1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15095, CVE-2017-7525

### Update Details

Risk is updated

## 22634 - Google Chrome Multiple Vulnerabilities Prior To 62.0.3202.62

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

### Update Details

Risk is updated

## 22635 - Google Chrome Multiple Vulnerabilities Prior To 62.0.3202.62

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

### Update Details

Risk is updated

## 130924 - Debian Linux 9.0 DSA-4020-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15396, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

### Update Details

Risk is updated



## 141760 - Red Hat Enterprise Linux RHSA-2017-2997 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

## 146035 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2902-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15396, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

## 146334 - SuSE Linux 42.3 openSUSE-SU-2018:0360-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6406

[Update Details](#)

Risk is updated

## 146402 - SuSE SLES 11 SP4 SUSE-SU-2018:0465-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000035

[Update Details](#)

Risk is updated

## 182492 - FreeBSD chromium Multiple Vulnerabilities (a692bffe-b6ad-11e7-a1c2-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

## 182539 - FreeBSD borgbackup Remote Users Can Override Repository Restrictions (0d369972-d4ba-11e7-

bfca-005056925db4)

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

Risk Level: Medium

CVE: CVE-2017-15914

[Update Details](#)

Risk is updated

192967 - Fedora Linux 27 FEDORA-2017-f2f3fa09e3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15398, CVE-2017-15399, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

193005 - Fedora Linux 25 FEDORA-2017-9015553e3d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

193008 - Fedora Linux 27 FEDORA-2017-15b815b9b7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

193027 - Fedora Linux 26 FEDORA-2017-4d90e9fc97 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15390, CVE-2017-15392, CVE-2017-15394, CVE-2017-15396, CVE-2017-15398, CVE-2017-5124, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5132, CVE-2017-5133

[Update Details](#)

Risk is updated

### 193049 - Fedora Linux 26 FEDORA-2017-7b0a42338c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15914

#### Update Details

Risk is updated

### 193057 - Fedora Linux 27 FEDORA-2017-81115c3047 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15914

#### Update Details

Risk is updated

### 193136 - Fedora Linux 26 FEDORA-2017-ea44f172e3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15386, CVE-2017-15387, CVE-2017-15388, CVE-2017-15389, CVE-2017-15390, CVE-2017-15391, CVE-2017-15392, CVE-2017-15393, CVE-2017-15394, CVE-2017-15395, CVE-2017-15398, CVE-2017-15399, CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427, CVE-2017-15429, CVE-2017-5124, CVE-2017-5125, CVE-2017-5126, CVE-2017-5127, CVE-2017-5128, CVE-2017-5129, CVE-2017-5130, CVE-2017-5131, CVE-2017-5132, CVE-2017-5133

#### Update Details

Risk is updated

### 23138 - LibreOffice Remote Arbitrary File Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 23139 - LibreOffice Remote Arbitrary File Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 131018 - Debian Linux 9.0 DSA-4111-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 146367 - SuSE SLED 12 SP2 SUSE-SU-2018:0428-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 146408 - SuSE Linux 42.3 openSUSE-SU-2018:0446-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 146417 - SuSE SLED 12 SP3 SUSE-SU-2018:0443-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6871

#### Update Details

Risk is updated

### 170923 - Amazon Linux AMI ALAS-2018-947 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15706

#### Update Details

Risk is updated

### 193249 - Fedora Linux 27 FEDORA-2018-0b48740047 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15706

[Update Details](#)

Risk is updated

193277 - Fedora Linux 26 FEDORA-2018-ac2e276c76 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15706

[Update Details](#)

Risk is updated

193290 - Fedora Linux 27 FEDORA-2018-3eb4d8e4c4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1055, CVE-2018-6871

[Update Details](#)

Risk is updated

131020 - Debian Linux 8.0, 9.0 DSA-4118-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15698

[Update Details](#)

Risk is updated

146366 - SuSE Linux 42.3 openSUSE-SU-2018:0419-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6612

[Update Details](#)

Risk is updated

193267 - Fedora Linux 26 FEDORA-2018-318b5d74bd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15698

[Update Details](#)

Risk is updated

193270 - Fedora Linux 27 FEDORA-2018-7b1517bc6e Update Is Not Installed

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

Risk Level: Medium  
CVE: CVE-2017-15698

[Update Details](#)

Risk is updated

146387 - SuSE Linux 42.3 openSUSE-SU-2018:0471-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-10689

[Update Details](#)

Risk is updated

186089 - Ubuntu Linux 14.04 USN-3567-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-10689

[Update Details](#)

Risk is updated

70086 - oracle.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

[Update Details](#)

FASLScript is updated

## DELETED CHECKS

4438 - Apache 2.0.x Multiple Denial-of-Service (Intrusive)

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

Risk Level: Medium

CVE: CVE-2004-0747, CVE-2004-0748, CVE-2004-0751, CVE-2004-0786, CVE-2004-0809

## ADDITIONAL NOTES

- 4438 - is deleted due to FP in certain situations.

## 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 2018 McAfee, Inc.

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