

## MCAFFEE FOUNDSTONE FSL UPDATE

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

### NEW CHECKS

#### 24634 - (JSA10916) Juniper Junos OS Libxml2 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449, CVE-2017-18258, CVE-2017-7375, CVE-2018-9251

#### Description

Multiple vulnerabilities are present in some versions of Juniper Junos OS.

#### Observation

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

Multiple vulnerabilities are present in some versions of Juniper Junos OS. The flaws lie in multiple components. Successful exploitation could allow an attacker to read arbitrary files, cause a denial of service condition in the target system, or possibly have unspecified other impact.

#### 147526 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0060-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20023, CVE-2018-20024, CVE-2018-6307

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0060-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005025.html>

SuSE SLES 12 SP3

x86\_64

libvncclient0-0.9.9-17.8.1

libvncserver0-0.9.9-17.8.1

LibVNCServer-debugsource-0.9.9-17.8.1

libvncserver0-debuginfo-0.9.9-17.8.1

libvncclient0-debuginfo-0.9.9-17.8.1

SuSE SLES 12 SP4

x86\_64

libvncclient0-0.9.9-17.8.1  
libvncserver0-0.9.9-17.8.1  
LibVNCServer-debugsource-0.9.9-17.8.1  
libvncserver0-debuginfo-0.9.9-17.8.1  
libvncclient0-debuginfo-0.9.9-17.8.1

### 147529 - SuSE SLES 11 SP4 SUSE-SU-2019:13927-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20024, CVE-2018-6307

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:13927-1

#### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005030.html>

SuSE SLES 11 SP4  
i586  
LibVNCServer-0.9.1-160.6.1

x86\_64  
LibVNCServer-0.9.1-160.6.1

### 147538 - SuSE Linux 42.3 openSUSE-SU-2019:0045-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20023, CVE-2018-20024, CVE-2018-6307

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0045-1

#### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00027.html>

SuSE Linux 42.3  
x86\_64  
LibVNCServer-devel-0.9.9-16.6.1  
linuxvnc-0.9.9-16.6.1

libvncclient0-0.9.9-16.6.1  
libvncserver0-0.9.9-16.6.1  
libvncclient0-debuginfo-0.9.9-16.6.1  
LibVNCServer-debugsource-0.9.9-16.6.1  
libvncserver0-debuginfo-0.9.9-16.6.1

linuxvnc-debuginfo-0.9.9-16.6.1

i586

LibVNCServer-devel-0.9.9-16.6.1

linuxvnc-0.9.9-16.6.1

libvncclient0-0.9.9-16.6.1

libvncserver0-0.9.9-16.6.1

libvncclient0-debuginfo-0.9.9-16.6.1

LibVNCServer-debugsource-0.9.9-16.6.1

libvncserver0-debuginfo-0.9.9-16.6.1

linuxvnc-debuginfo-0.9.9-16.6.1

## 147539 - SuSE SLED 15 SUSE-SU-2019:0080-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20023, CVE-2018-20024, CVE-2018-6307

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0080-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005032.html>

SuSE SLED 15

x86\_64

libvncclient0-0.9.10-4.3.1

libvncclient0-debuginfo-0.9.10-4.3.1

LibVNCServer-debugsource-0.9.10-4.3.1

## 194652 - Fedora Linux 29 FEDORA-2019-18b3a10c7f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15686, CVE-2018-15687, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-18b3a10c7f

### 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/2019/1/?count=200&page=1>

Fedora Core 29

systemd-239-8.gite339eae.fc29

## 194654 - Fedora Linux 28 FEDORA-2019-337484d88b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3701

### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-337484d88b

### 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/2019/1/?count=200&page=1>

Fedora Core 28

kernel-headers-4.19.14-200.fc28

kernel-tools-4.19.14-200.fc28

kernel-4.19.14-200.fc28

## 147546 - SuSE SLES 12 SP3 SUSE-SU-2019:0095-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14613, CVE-2018-14617, CVE-2018-14633, CVE-2018-16276, CVE-2018-16597, CVE-2018-17182, CVE-2018-18281, CVE-2018-18386, CVE-2018-18690, CVE-2018-18710, CVE-2018-7480, CVE-2018-7757, CVE-2018-9516

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0095-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005035.html>

SuSE SLES 12 SP3

x86\_64

kernel-azure-4.4.162-4.19.2

kernel-azure-base-4.4.162-4.19.2

kernel-azure-base-debuginfo-4.4.162-4.19.2

kernel-azure-debugsource-4.4.162-4.19.2

kernel-azure-devel-4.4.162-4.19.2

kernel-syms-azure-4.4.162-4.19.1

kernel-azure-debuginfo-4.4.162-4.19.2

noarch

kernel-devel-azure-4.4.162-4.19.1

kernel-source-azure-4.4.162-4.19.1

## 24525 - (MSPT-Dec2018) Microsoft PowerPoint Improperly Handles Objects in Memory Remote Code Execution (CVE-2018-8628)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-8628

### Description

A vulnerability in some versions of Microsoft PowerPoint could lead to remote code execution.

### Observation

A vulnerability in some versions of Microsoft PowerPoint could lead to remote code execution.

The flaw lies in the Improperly Handles Objects in Memory component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

## 24628 - (MSPT-Dec2018) Microsoft Excel Improperly Handles Objects in Memory Remote Code Execution (CVE-2018-8597)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-8597

### Description

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

### Observation

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

The flaw lies in the Improperly Handles Objects in Memory component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

## 24636 - (SB10264) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-11784, CVE-2018-12327, CVE-2018-7170, CVE-2019-3581

### Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

### Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaw lies in multiple components. Successful exploitation could allow an attacker to bypass certain security restrictions, perform some unauthorized actions, cause a denial of service or execute arbitrary code.

## 88995 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-013-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18205, CVE-2017-18206, CVE-2018-1071, CVE-2018-1083, CVE-2018-1100, CVE-2018-7548, CVE-2018-7549

### Description

The scan detected that the host is missing the following update:  
SSA:2019-013-01

### 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=2019&m=slackware-security.407621>

Slackware 14.0  
x86\_64  
zsh-5.6.2-x86\_64-1

Slackware 14.2  
x86\_64  
zsh-5.6.2-x86\_64-1

i586  
zsh-5.6.2-i586-1

Slackware 14.1  
x86\_64  
zsh-5.6.2-x86\_64-1

## **88996 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-011-01 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, CVE-2019-5882

### Description

The scan detected that the host is missing the following update:  
SSA:2019-011-01

### 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=2019&m=slackware-security.478665>

Slackware 14.0  
x86\_64  
irssi-1.1.2-x86\_64-1

Slackware 14.2  
x86\_64  
irssi-1.1.2-x86\_64-1

i586  
irssi-1.1.2-i586-1

Slackware 14.1  
x86\_64  
irssi-1.1.2-x86\_64-1

## 131274 - Debian Linux 9.0 DSA-4369-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19961, CVE-2018-19962, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967

### Description

The scan detected that the host is missing the following update:  
DSA-4369-1

### Observation

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

<http://www.debian.org/security/2019/dsa-4369>

Debian 9.0

all

xen-hypervisor-4.8-armhf\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-system-arm64\_4.8.5+shim4.10.2+xsa282-1+deb9u11

libxen-dev\_4.8.5+shim4.10.2+xsa282-1+deb9u11

libxenstore3.0\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-system-armhf\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-utils-common\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-hypervisor-4.8-amd64\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-system-amd64\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-utils-4.8\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xen-hypervisor-4.8-arm64\_4.8.5+shim4.10.2+xsa282-1+deb9u11

xenstore-utils\_4.8.5+shim4.10.2+xsa282-1+deb9u11

libxen-4.8\_4.8.5+shim4.10.2+xsa282-1+deb9u11

## 147525 - SuSE Linux 15.0 openSUSE-SU-2019:0009-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19295

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0009-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00008.html>

SuSE Linux 15.0

x86\_64

singularity-debugsource-2.6.1-lp150.2.6.1

singularity-devel-2.6.1-lp150.2.6.1

libsingularity1-debuginfo-2.6.1-lp150.2.6.1

singularity-2.6.1-lp150.2.6.1

singularity-debuginfo-2.6.1-lp150.2.6.1

libsingularity1-2.6.1-lp150.2.6.1

## 147527 - SuSE Linux 15.0 openSUSE-SU-2019:0010-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19788

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0010-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00010.html>

SuSE Linux 15.0

i586

polkit-debugsource-0.114-lp150.2.6.1

libpolkit0-0.114-lp150.2.6.1

polkit-0.114-lp150.2.6.1

polkit-debuginfo-0.114-lp150.2.6.1

polkit-devel-0.114-lp150.2.6.1

typelib-1\_0-Polkit-1\_0-0.114-lp150.2.6.1

polkit-devel-debuginfo-0.114-lp150.2.6.1

libpolkit0-debuginfo-0.114-lp150.2.6.1

noarch

polkit-doc-0.114-lp150.2.6.1

x86\_64

polkit-debugsource-0.114-lp150.2.6.1

libpolkit0-0.114-lp150.2.6.1

libpolkit0-32bit-0.114-lp150.2.6.1

polkit-0.114-lp150.2.6.1

polkit-debuginfo-0.114-lp150.2.6.1

polkit-devel-0.114-lp150.2.6.1

typelib-1\_0-Polkit-1\_0-0.114-lp150.2.6.1

polkit-devel-debuginfo-0.114-lp150.2.6.1

libpolkit0-32bit-debuginfo-0.114-lp150.2.6.1

libpolkit0-debuginfo-0.114-lp150.2.6.1

## 147528 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0048-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5882

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0048-1

### Observation

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



<https://lists.opensuse.org/opensuse-updates/2019-01/msg00051.html>

SuSE Linux 15.0

x86\_64

irssi-debuginfo-1.1.2-lp150.2.4.1

irssi-devel-1.1.2-lp150.2.4.1

irssi-debugsource-1.1.2-lp150.2.4.1

irssi-1.1.2-lp150.2.4.1

SuSE Linux 42.3

x86\_64

irssi-devel-1.1.2-29.1

irssi-1.1.2-29.1

irssi-debuginfo-1.1.2-29.1

irssi-debugsource-1.1.2-29.1

i586

irssi-devel-1.1.2-29.1

irssi-1.1.2-29.1

irssi-debuginfo-1.1.2-29.1

irssi-debugsource-1.1.2-29.1

### 147532 - SuSE Linux 15.0 openSUSE-SU-2019:0020-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000858

#### Description

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

openSUSE-SU-2019:0020-1

#### Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00024.html>

SuSE Linux 15.0

i586

gpg2-debuginfo-2.2.5-lp150.3.6.1

gpg2-debugsource-2.2.5-lp150.3.6.1

gpg2-2.2.5-lp150.3.6.1

noarch

gpg2-lang-2.2.5-lp150.3.6.1

x86\_64

gpg2-debuginfo-2.2.5-lp150.3.6.1

gpg2-debugsource-2.2.5-lp150.3.6.1

gpg2-2.2.5-lp150.3.6.1

### 147535 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0050-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3500

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0050-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00047.html>

SuSE Linux 15.0

x86\_64

aria2-1.33.1-lp150.2.4.1

aria2-devel-1.33.1-lp150.2.4.1

libaria2-0-1.33.1-lp150.2.4.1

libaria2-0-debuginfo-1.33.1-lp150.2.4.1

aria2-debuginfo-1.33.1-lp150.2.4.1

aria2-debugsource-1.33.1-lp150.2.4.1

noarch

aria2-lang-1.33.1-lp150.2.4.1

aria2-1.33.1-bp150.3.7.1

aria2-devel-1.33.1-bp150.3.7.1

libaria2-0-1.33.1-bp150.3.7.1

SuSE Linux 42.3

i586

libaria2-0-debuginfo-1.24.0-4.4.1

libaria2-0-1.24.0-4.4.1

aria2-1.24.0-4.4.1

aria2-debugsource-1.24.0-4.4.1

aria2-devel-1.24.0-4.4.1

aria2-debuginfo-1.24.0-4.4.1

noarch

aria2-lang-1.24.0-4.4.1

x86\_64

libaria2-0-debuginfo-1.24.0-4.4.1

libaria2-0-1.24.0-4.4.1

aria2-1.24.0-4.4.1

aria2-debugsource-1.24.0-4.4.1

aria2-devel-1.24.0-4.4.1

aria2-debuginfo-1.24.0-4.4.1

**147541 - SuSE Linux 15.0 openSUSE-SU-2019:0044-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2018-20102, CVE-2018-20103

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0044-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00025.html>

SuSE Linux 15.0  
x86\_64  
haproxy-debugsource-1.8.15~git0.6b6a350a-lp150.2.6.1  
haproxy-1.8.15~git0.6b6a350a-lp150.2.6.1  
haproxy-debuginfo-1.8.15~git0.6b6a350a-lp150.2.6.1

### **147543 - SuSE Linux 42.3 openSUSE-SU-2019:0021-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2018-19456

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0021-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00016.html>

SuSE Linux 42.3  
x86\_64  
libgit2-debugsource-0.24.1-10.6.1  
libgit2-24-32bit-0.24.1-10.6.1  
libgit2-24-debuginfo-0.24.1-10.6.1  
libgit2-24-0.24.1-10.6.1  
libgit2-24-debuginfo-32bit-0.24.1-10.6.1  
libgit2-devel-0.24.1-10.6.1

i586  
libgit2-24-debuginfo-0.24.1-10.6.1  
libgit2-24-0.24.1-10.6.1  
libgit2-debugsource-0.24.1-10.6.1  
libgit2-devel-0.24.1-10.6.1

### **147544 - SuSE Linux 15.0 openSUSE-SU-2019:0008-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2018-5804, CVE-2018-5813, CVE-2018-5815, CVE-2018-5816

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0008-1

### Observation

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

For more information see:

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00009.html>

SuSE Linux 15.0

x86\_64

libraw-tools-0.18.9-lp150.2.3.1

libraw-tools-debuginfo-0.18.9-lp150.2.3.1

libraw16-debuginfo-0.18.9-lp150.2.3.1

libraw-devel-0.18.9-lp150.2.3.1

libraw-debuginfo-0.18.9-lp150.2.3.1

libraw-debugsource-0.18.9-lp150.2.3.1

libraw-devel-static-0.18.9-lp150.2.3.1

libraw16-0.18.9-lp150.2.3.1

i586

libraw-tools-0.18.9-lp150.2.3.1

libraw-tools-debuginfo-0.18.9-lp150.2.3.1

libraw16-debuginfo-0.18.9-lp150.2.3.1

libraw-devel-0.18.9-lp150.2.3.1

libraw-debuginfo-0.18.9-lp150.2.3.1

libraw-debugsource-0.18.9-lp150.2.3.1

libraw-devel-static-0.18.9-lp150.2.3.1

libraw16-0.18.9-lp150.2.3.1

## 160503 - CentOS 7 CESA-2019-0049 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15688, CVE-2018-16864, CVE-2018-16865

### Description

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

CESA-2019-0049

### Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2019-January/023143.html>

CentOS 7

x86\_64

systemd-219-62.el7\_6.2

systemd-devel-219-62.el7\_6.2

libgudev1-devel-219-62.el7\_6.2

libgudev1-219-62.el7\_6.2

systemd-sysv-219-62.el7\_6.2

systemd-resolved-219-62.el7\_6.2

systemd-python-219-62.el7\_6.2

systemd-libs-219-62.el7\_6.2

systemd-journal-gateway-219-62.el7\_6.2

systemd-networkd-219-62.el7\_6.2

i686

systemd-resolved-219-62.el7\_6.2

libgudev1-219-62.el7\_6.2

systemd-libs-219-62.el7\_6.2

systemd-devel-219-62.el7\_6.2  
libgudev1-devel-219-62.el7\_6.2

## 163784 - Oracle Enterprise Linux ELSA-2019-4510 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1094, CVE-2018-19824

### Description

The scan detected that the host is missing the following update:  
ELSA-2019-4510

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-January/008371.html>  
<http://oss.oracle.com/pipermail/el-errata/2019-January/008372.html>

OEL7  
x86\_64  
kernel-uek-debug-4.1.12-124.24.3.el7uek  
kernel-uek-4.1.12-124.24.3.el7uek  
kernel-uek-devel-4.1.12-124.24.3.el7uek  
kernel-uek-firmware-4.1.12-124.24.3.el7uek  
kernel-uek-debug-devel-4.1.12-124.24.3.el7uek  
kernel-uek-doc-4.1.12-124.24.3.el7uek

OEL6  
x86\_64  
kernel-uek-doc-4.1.12-124.24.3.el6uek  
kernel-uek-4.1.12-124.24.3.el6uek  
kernel-uek-debug-4.1.12-124.24.3.el6uek  
kernel-uek-devel-4.1.12-124.24.3.el6uek  
kernel-uek-firmware-4.1.12-124.24.3.el6uek  
kernel-uek-debug-devel-4.1.12-124.24.3.el6uek

## 163785 - Oracle Enterprise Linux ELSA-2019-0059 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15127

### Description

The scan detected that the host is missing the following update:  
ELSA-2019-0059

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-January/008368.html>

OEL7  
x86\_64

libvncserver-devel-0.9.9-13.el7\_6  
libvncserver-0.9.9-13.el7\_6

### 163786 - Oracle Enterprise Linux ELSA-2019-0049 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15688, CVE-2018-16864, CVE-2018-16865

#### Description

The scan detected that the host is missing the following update:  
ELSA-2019-0049

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2019-January/008367.html>

OEL7  
x86\_64  
libgudev1-devel-219-62.0.4.el7\_6.2  
systemd-resolved-219-62.0.4.el7\_6.2  
systemd-devel-219-62.0.4.el7\_6.2  
systemd-219-62.0.4.el7\_6.2  
systemd-libs-219-62.0.4.el7\_6.2  
libgudev1-219-62.0.4.el7\_6.2  
systemd-networkd-219-62.0.4.el7\_6.2  
systemd-journal-gateway-219-62.0.4.el7\_6.2  
systemd-python-219-62.0.4.el7\_6.2  
systemd-sysv-219-62.0.4.el7\_6.2

### 182885 - FreeBSD irssi Use After Free (d38bbb79-14f3-11e9-9ce2-28d244aee256)

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

Risk Level: High

CVE: CVE-2019-5882

#### Description

The scan detected that the host is missing the following update:  
irssi -- Use after free (d38bbb79-14f3-11e9-9ce2-28d244aee256)

#### Observation

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

<http://www.vuxml.org/freebsd/d38bbb79-14f3-11e9-9ce2-28d244aee256.html>

Affected packages:

1.1.0,1 <= irssi < 1.1.2,1

### 196231 - Red Hat Enterprise Linux RHSA-2019-0059 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15127

#### Description

The scan detected that the host is missing the following update:  
RHSA-2019-0059

#### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-January/msg00008.html>

#### RHEL7D

x86\_64  
libvncserver-devel-0.9.9-13.el7\_6  
libvncserver-0.9.9-13.el7\_6  
libvncserver-debuginfo-0.9.9-13.el7\_6

#### RHEL7S

x86\_64  
libvncserver-devel-0.9.9-13.el7\_6  
libvncserver-0.9.9-13.el7\_6  
libvncserver-debuginfo-0.9.9-13.el7\_6

#### RHEL7WS

x86\_64  
libvncserver-devel-0.9.9-13.el7\_6  
libvncserver-0.9.9-13.el7\_6  
libvncserver-debuginfo-0.9.9-13.el7\_6

### 196232 - Red Hat Enterprise Linux RHSA-2019-0049 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15688, CVE-2018-16864, CVE-2018-16865

#### Description

The scan detected that the host is missing the following update:  
RHSA-2019-0049

#### Observation

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

<http://www.redhat.com/archives/rhsa-announce/2019-January/msg00007.html>

#### RHEL7D

x86\_64  
systemd-219-62.el7\_6.2  
systemd-devel-219-62.el7\_6.2  
libgudev1-devel-219-62.el7\_6.2  
libgudev1-219-62.el7\_6.2  
systemd-sysv-219-62.el7\_6.2  
systemd-resolved-219-62.el7\_6.2  
systemd-journal-gateway-219-62.el7\_6.2  
systemd-libs-219-62.el7\_6.2  
systemd-python-219-62.el7\_6.2

systemd-networkd-219-62.el7\_6.2  
systemd-debuginfo-219-62.el7\_6.2

#### RHEL7S

x86\_64  
systemd-219-62.el7\_6.2  
systemd-devel-219-62.el7\_6.2  
libgudev1-devel-219-62.el7\_6.2  
libgudev1-219-62.el7\_6.2  
systemd-sysv-219-62.el7\_6.2  
systemd-resolved-219-62.el7\_6.2  
systemd-journal-gateway-219-62.el7\_6.2  
systemd-libs-219-62.el7\_6.2  
systemd-python-219-62.el7\_6.2  
systemd-networkd-219-62.el7\_6.2  
systemd-debuginfo-219-62.el7\_6.2

#### RHEL7WS

x86\_64  
systemd-219-62.el7\_6.2  
systemd-devel-219-62.el7\_6.2  
libgudev1-devel-219-62.el7\_6.2  
libgudev1-219-62.el7\_6.2  
systemd-sysv-219-62.el7\_6.2  
systemd-resolved-219-62.el7\_6.2  
systemd-journal-gateway-219-62.el7\_6.2  
systemd-libs-219-62.el7\_6.2  
systemd-python-219-62.el7\_6.2  
systemd-networkd-219-62.el7\_6.2  
systemd-debuginfo-219-62.el7\_6.2

### 24635 - (JSA10895) Juniper Junos OS Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0060

#### Description

A vulnerability is present in some versions of Juniper Junos.

#### Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in device control daemon process. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

### 131272 - Debian Linux 9.0 DSA-4366-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19857

#### Description

The scan detected that the host is missing the following update:  
DSA-4366-1



## Observation

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

<http://www.debian.org/security/2019/dsa-4366>

Debian 9.0  
all  
vlc\_3.0.6-0+deb9u1

## **147524 - SuSE Linux 42.3 openSUSE-SU-2019:0042-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-13785, CVE-2018-16435, CVE-2018-2938, CVE-2018-2940, CVE-2018-2952, CVE-2018-2973, CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3169, CVE-2018-3180, CVE-2018-3214, CVE-2018-3639

## Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0042-1

## Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00030.html>

SuSE Linux 42.3

i586  
java-1\_7\_0-openjdk-bootstrap-devel-1.7.0.201-54.1  
java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-headless-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-devel-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-1.7.0.201-54.1  
java-1\_7\_0-openjdk-src-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-headless-1.7.0.201-54.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-debugsource-1.7.0.201-54.1  
java-1\_7\_0-openjdk-devel-1.7.0.201-54.1  
java-1\_7\_0-openjdk-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-headless-1.7.0.201-54.1  
java-1\_7\_0-openjdk-demo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-debugsource-1.7.0.201-54.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-accessibility-1.7.0.201-54.1

noarch

java-1\_7\_0-openjdk-javadoc-1.7.0.201-54.1

x86\_64

java-1\_7\_0-openjdk-bootstrap-devel-1.7.0.201-54.1  
java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-headless-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-devel-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-1.7.0.201-54.1  
java-1\_7\_0-openjdk-src-1.7.0.201-54.1

java-1\_7\_0-openjdk-bootstrap-headless-1.7.0.201-54.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-debugsource-1.7.0.201-54.1  
java-1\_7\_0-openjdk-devel-1.7.0.201-54.1  
java-1\_7\_0-openjdk-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-headless-1.7.0.201-54.1  
java-1\_7\_0-openjdk-demo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-bootstrap-debugsource-1.7.0.201-54.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.201-54.1  
java-1\_7\_0-openjdk-accessibility-1.7.0.201-54.1

## 147530 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0049-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13785, CVE-2018-16435, CVE-2018-2938, CVE-2018-2940, CVE-2018-2952, CVE-2018-2973, CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3169, CVE-2018-3180, CVE-2018-3214, CVE-2018-3639

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0049-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005021.html>

#### SuSE SLED 12 SP3

x86\_64  
java-1\_7\_0-openjdk-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-debugsource-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-43.18.1

#### SuSE SLED 12 SP4

x86\_64  
java-1\_7\_0-openjdk-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-debugsource-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-43.18.1

#### SuSE SLES 12 SP4

x86\_64  
java-1\_7\_0-openjdk-debugsource-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-demo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-debuginfo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-devel-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.201-43.18.1  
java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-43.18.1

SuSE SLES 12 SP3

x86\_64

java-1\_7\_0-openjdk-debugsource-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-demo-debuginfo-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-demo-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-debuginfo-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-headless-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-devel-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-devel-debuginfo-1.7.0.201-43.18.1

java-1\_7\_0-openjdk-headless-debuginfo-1.7.0.201-43.18.1

## 147533 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0057-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13785, CVE-2018-16435, CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3169, CVE-2018-3180, CVE-2018-3183, CVE-2018-3214

### Description

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

SUSE-SU-2019:0057-1

### Observation

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

For more information see:

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005026.html>

SuSE SLED 12 SP3

x86\_64

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-headless-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-debugsource-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-27.29.1

SuSE SLED 12 SP4

x86\_64

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-headless-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-debugsource-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-27.29.1

SuSE SLES 12 SP4

x86\_64

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-devel-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-headless-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-debugsource-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-demo-1.8.0.191-27.29.1

java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-27.29.1

SuSE SLES 12 SP3

x86\_64  
java-1\_8\_0-openjdk-debuginfo-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-devel-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-headless-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-debugsource-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-demo-1.8.0.191-27.29.1  
java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-27.29.1

## 147542 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0059-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4191, CVE-2018-4197, CVE-2018-4207, CVE-2018-4208, CVE-2018-4209, CVE-2018-4210, CVE-2018-4212, CVE-2018-4213, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4345, CVE-2018-4358, CVE-2018-4359, CVE-2018-4361, CVE-2018-4372, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4416

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0059-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005029.html>

### SuSE SLES 12 SP3

x86\_64  
webkit2gtk3-debugsource-2.22.4-2.29.3  
typelib-1\_0-JavaScriptCore-4\_0-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-debuginfo-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-debuginfo-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-debuginfo-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-2.22.4-2.29.3  
typelib-1\_0-WebKit2-4\_0-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-2.22.4-2.29.3

### SuSE SLES 12 SP4

x86\_64  
webkit2gtk3-debugsource-2.22.4-2.29.3  
typelib-1\_0-JavaScriptCore-4\_0-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-debuginfo-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-debuginfo-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-debuginfo-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-2.22.4-2.29.3  
typelib-1\_0-WebKit2-4\_0-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-2.22.4-2.29.3

### SuSE SLED 12 SP4

x86\_64  
webkit2gtk3-debugsource-2.22.4-2.29.3  
typelib-1\_0-JavaScriptCore-4\_0-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-debuginfo-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-debuginfo-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-debuginfo-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-2.22.4-2.29.3  
typelib-1\_0-WebKit2-4\_0-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-2.22.4-2.29.3

noarch  
libwebkit2gtk3-lang-2.22.4-2.29.3

SuSE SLED 12 SP3

x86\_64  
webkit2gtk3-debugsource-2.22.4-2.29.3  
typelib-1\_0-JavaScriptCore-4\_0-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-debuginfo-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-debuginfo-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-debuginfo-2.22.4-2.29.3  
webkit2gtk-4\_0-injected-bundles-2.22.4-2.29.3  
libwebkit2gtk-4\_0-37-2.22.4-2.29.3  
typelib-1\_0-WebKit2-4\_0-2.22.4-2.29.3  
libjavascriptcoregtk-4\_0-18-2.22.4-2.29.3

noarch  
libwebkit2gtk3-lang-2.22.4-2.29.3

## 147545 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0043-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13785, CVE-2018-16435, CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3169, CVE-2018-3180, CVE-2018-3183, CVE-2018-3214

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0043-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00018.html>

SuSE Linux 15.0

i586  
java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-devel-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-accessibility-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-debuginfo-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-debugsource-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-demo-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-lp150.2.9.2  
java-1\_8\_0-openjdk-src-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-headless-1.8.0.191-lp150.2.9.2

noarch

java-1\_8\_0-openjdk-javadoc-1.8.0.191-lp150.2.9.2

x86\_64

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-devel-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-accessibility-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-debugsource-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-demo-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-src-1.8.0.191-lp150.2.9.2

java-1\_8\_0-openjdk-headless-1.8.0.191-lp150.2.9.2

SuSE Linux 42.3

i586

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-headless-1.8.0.191-30.1

java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-debugsource-1.8.0.191-30.1

java-1\_8\_0-openjdk-devel-1.8.0.191-30.1

java-1\_8\_0-openjdk-src-1.8.0.191-30.1

java-1\_8\_0-openjdk-1.8.0.191-30.1

java-1\_8\_0-openjdk-accessibility-1.8.0.191-30.1

java-1\_8\_0-openjdk-demo-1.8.0.191-30.1

java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-30.1

noarch

java-1\_8\_0-openjdk-javadoc-1.8.0.191-30.1

x86\_64

java-1\_8\_0-openjdk-headless-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-headless-1.8.0.191-30.1

java-1\_8\_0-openjdk-devel-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-debugsource-1.8.0.191-30.1

java-1\_8\_0-openjdk-devel-1.8.0.191-30.1

java-1\_8\_0-openjdk-src-1.8.0.191-30.1

java-1\_8\_0-openjdk-1.8.0.191-30.1

java-1\_8\_0-openjdk-accessibility-1.8.0.191-30.1

java-1\_8\_0-openjdk-demo-1.8.0.191-30.1

java-1\_8\_0-openjdk-demo-debuginfo-1.8.0.191-30.1

java-1\_8\_0-openjdk-debuginfo-1.8.0.191-30.1

## 147547 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0096-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17097, CVE-2018-17098

### Description

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

SUSE-SU-2019:0096-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005036.html>

### SuSE SLES 12 SP3

x86\_64  
soundtouch-debugsource-1.7.1-5.11.1  
libSoundTouch0-1.7.1-5.11.1  
soundtouch-debuginfo-1.7.1-5.11.1  
libSoundTouch0-debuginfo-1.7.1-5.11.1

### SuSE SLES 12 SP4

x86\_64  
soundtouch-debugsource-1.7.1-5.11.1  
libSoundTouch0-1.7.1-5.11.1  
soundtouch-debuginfo-1.7.1-5.11.1  
libSoundTouch0-debuginfo-1.7.1-5.11.1

### SuSE SLED 12 SP4

x86\_64  
libSoundTouch0-1.7.1-5.11.1  
libSoundTouch0-32bit-1.7.1-5.11.1  
libSoundTouch0-debuginfo-32bit-1.7.1-5.11.1  
libSoundTouch0-debuginfo-1.7.1-5.11.1  
soundtouch-1.7.1-5.11.1  
soundtouch-debugsource-1.7.1-5.11.1  
soundtouch-debuginfo-1.7.1-5.11.1

### SuSE SLED 12 SP3

x86\_64  
libSoundTouch0-1.7.1-5.11.1  
libSoundTouch0-32bit-1.7.1-5.11.1  
libSoundTouch0-debuginfo-32bit-1.7.1-5.11.1  
libSoundTouch0-debuginfo-1.7.1-5.11.1  
soundtouch-1.7.1-5.11.1  
soundtouch-debugsource-1.7.1-5.11.1  
soundtouch-debuginfo-1.7.1-5.11.1

## 171059 - Amazon Linux AMI ALAS-2019-1146 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14679, CVE-2018-14680, CVE-2018-14681, CVE-2018-14682, CVE-2018-15378

### Description

The scan detected that the host is missing the following update:  
ALAS-2019-1146

### Observation

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

<https://alas.aws.amazon.com/ALAS-2019-1146.html>

Amazon Linux AMI  
i686

clamav-0.100.2-2.35.amzn1  
clamav-milter-0.100.2-2.35.amzn1  
clamav-devel-0.100.2-2.35.amzn1  
clamd-0.100.2-2.35.amzn1  
clamav-lib-0.100.2-2.35.amzn1  
clamav-debuginfo-0.100.2-2.35.amzn1  
clamav-update-0.100.2-2.35.amzn1  
clamav-db-0.100.2-2.35.amzn1

noarch  
clamav-filesystem-0.100.2-2.35.amzn1  
clamav-data-0.100.2-2.35.amzn1

x86\_64  
clamav-0.100.2-2.35.amzn1  
clamav-milter-0.100.2-2.35.amzn1  
clamav-devel-0.100.2-2.35.amzn1  
clamd-0.100.2-2.35.amzn1  
clamav-lib-0.100.2-2.35.amzn1  
clamav-debuginfo-0.100.2-2.35.amzn1  
clamav-update-0.100.2-2.35.amzn1  
clamav-db-0.100.2-2.35.amzn1

### 24483 - (SB10257) McAfee ePolicy Orchestrator Tomcat Vulnerability

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

Risk Level: Medium

CVE: CVE-2018-11784

#### Description

A vulnerability is present in some versions of McAfee ePolicy Orchestrator.

#### Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

A vulnerability is present in some versions of McAfee ePolicy Orchestrator. The flaw lies in the ePO web core services. Successful exploitation could allow an attacker to retrieve sensitive data from the target system or may aid in phishing attacks.

### 24629 - (MSPT-Dec2018) Microsoft Excel Reads Out of Bound Memory Information Disclosure (CVE-2018-8627)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-8627

#### Description

A vulnerability in some versions of Microsoft Excel could lead to information disclosure.

#### Observation

A vulnerability in some versions of Microsoft Excel could lead to information disclosure.

The flaw lies in the Reads Out of Bound Memory component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

### 24630 - IBM DB2 Privilege Escalation Vulnerability (ibm10733122)



Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-1802

#### Description

A vulnerability is present in some versions of IBM DB2.

#### Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to loading libraries from an untrusted path. Successful exploitation could allow a local attacker to gain full access to the DB2 instance account.

### **24639 - (JSA10894) Juniper ScreenOS Stored Cross-site Scripting Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0059

#### Description

A vulnerability is present in some versions of Juniper ScreenOS.

#### Observation

Juniper ScreenOS is an operating system used in Juniper firewall and VPN.

A vulnerability is present in some versions of Juniper ScreenOS. The flaw lies in graphical user interface of ScreenOS. Successful exploitation could allow an attacker to retrieve sensitive information from the target system.

### **24644 - Oracle Java SE Critical Patch Update January 2019**

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

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2019-2422, CVE-2019-2426, CVE-2019-2449

#### Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

#### Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to have unauthorized read access to Java SE accessible data and cause a denial of service condition on the targeted system.

### **147534 - SuSE Linux 42.3 openSUSE-SU-2019:0051-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-10852

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0051-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00045.html>

SuSE Linux 42.3

x86\_64

sssd-debuginfo-1.13.4-12.1  
sssd-krb5-common-1.13.4-12.1  
libsss\_sudo-debuginfo-1.13.4-12.1  
sssd-proxy-debuginfo-1.13.4-12.1  
sssd-tools-1.13.4-12.1  
sssd-32bit-1.13.4-12.1  
sssd-debuginfo-32bit-1.13.4-12.1  
sssd-krb5-common-debuginfo-1.13.4-12.1  
sssd-ad-debuginfo-1.13.4-12.1  
libipa\_hbac-devel-1.13.4-12.1  
libsss\_idmap0-1.13.4-12.1  
python-sss\_nss\_idmap-debuginfo-1.13.4-12.1  
python-ipa\_hbac-debuginfo-1.13.4-12.1  
sssd-krb5-debuginfo-1.13.4-12.1  
libsss\_nss\_idmap0-1.13.4-12.1  
sssd-ldap-1.13.4-12.1  
python-sssd-config-debuginfo-1.13.4-12.1  
libipa\_hbac0-debuginfo-1.13.4-12.1  
sssd-debugsource-1.13.4-12.1  
sssd-ldap-debuginfo-1.13.4-12.1  
sssd-tools-debuginfo-1.13.4-12.1  
sssd-krb5-1.13.4-12.1  
python-ipa\_hbac-1.13.4-12.1  
libsss\_nss\_idmap-devel-1.13.4-12.1  
sssd-ipa-1.13.4-12.1  
libsss\_idmap-devel-1.13.4-12.1  
sssd-ipa-debuginfo-1.13.4-12.1  
libipa\_hbac0-1.13.4-12.1  
sssd-ad-1.13.4-12.1  
libsss\_nss\_idmap0-debuginfo-1.13.4-12.1  
python-sssd-config-1.13.4-12.1  
libsss\_sudo-1.13.4-12.1  
libsss\_idmap0-debuginfo-1.13.4-12.1  
sssd-proxy-1.13.4-12.1  
python-sss\_nss\_idmap-1.13.4-12.1  
sssd-1.13.4-12.1

i586

sssd-debuginfo-1.13.4-12.1  
sssd-krb5-common-1.13.4-12.1  
libsss\_sudo-debuginfo-1.13.4-12.1  
sssd-proxy-debuginfo-1.13.4-12.1  
sssd-tools-1.13.4-12.1  
sssd-krb5-common-debuginfo-1.13.4-12.1  
sssd-ad-debuginfo-1.13.4-12.1  
libipa\_hbac-devel-1.13.4-12.1  
libsss\_idmap0-1.13.4-12.1  
python-sss\_nss\_idmap-debuginfo-1.13.4-12.1  
python-ipa\_hbac-debuginfo-1.13.4-12.1

sssd-krb5-debuginfo-1.13.4-12.1  
libsss\_nss\_idmap0-1.13.4-12.1  
sssd-ldap-1.13.4-12.1  
python-sssd-config-debuginfo-1.13.4-12.1  
libipa\_hbac0-debuginfo-1.13.4-12.1  
sssd-debugsource-1.13.4-12.1  
sssd-ldap-debuginfo-1.13.4-12.1  
sssd-tools-debuginfo-1.13.4-12.1  
sssd-krb5-1.13.4-12.1  
python-ipa\_hbac-1.13.4-12.1  
libsss\_nss\_idmap-devel-1.13.4-12.1  
sssd-ipa-1.13.4-12.1  
libsss\_idmap-devel-1.13.4-12.1  
sssd-ipa-debuginfo-1.13.4-12.1  
libipa\_hbac0-1.13.4-12.1  
sssd-ad-1.13.4-12.1  
libsss\_nss\_idmap0-debuginfo-1.13.4-12.1  
python-sssd-config-1.13.4-12.1  
libsss\_sudo-1.13.4-12.1  
libsss\_idmap0-debuginfo-1.13.4-12.1  
sssd-proxy-1.13.4-12.1  
python-sss\_nss\_idmap-1.13.4-12.1  
sssd-1.13.4-12.1

## 147537 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0081-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10852

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2019:0081-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2019-January/005031.html>

SuSE SLED 12 SP3

x86\_64

sssd-ldap-debuginfo-1.13.4-34.23.1  
libsss\_sudo-debuginfo-1.13.4-34.23.1  
sssd-32bit-1.13.4-34.23.1  
sssd-1.13.4-34.23.1  
libipa\_hbac0-debuginfo-1.13.4-34.23.1  
libsss\_sudo-1.13.4-34.23.1  
libipa\_hbac0-1.13.4-34.23.1  
libsss\_idmap0-1.13.4-34.23.1  
sssd-ad-1.13.4-34.23.1  
libsss\_nss\_idmap0-1.13.4-34.23.1  
sssd-krb5-common-debuginfo-1.13.4-34.23.1  
python-sssd-config-debuginfo-1.13.4-34.23.1  
sssd-tools-debuginfo-1.13.4-34.23.1  
sssd-debugsource-1.13.4-34.23.1  
sssd-proxy-debuginfo-1.13.4-34.23.1  
libsss\_nss\_idmap0-debuginfo-1.13.4-34.23.1

sssd-krb5-common-1.13.4-34.23.1  
sssd-ipa-1.13.4-34.23.1  
sssd-krb5-debuginfo-1.13.4-34.23.1  
sssd-ad-debuginfo-1.13.4-34.23.1  
sssd-proxy-1.13.4-34.23.1  
sssd-tools-1.13.4-34.23.1  
sssd-debuginfo-32bit-1.13.4-34.23.1  
sssd-ldap-1.13.4-34.23.1  
python-sssd-config-1.13.4-34.23.1  
libsss\_idmap0-debuginfo-1.13.4-34.23.1  
sssd-debuginfo-1.13.4-34.23.1  
sssd-krb5-1.13.4-34.23.1  
sssd-ipa-debuginfo-1.13.4-34.23.1

SuSE SLES 12 SP3

x86\_64

sssd-ldap-debuginfo-1.13.4-34.23.1  
libsss\_sudo-debuginfo-1.13.4-34.23.1  
python-sssd-config-1.13.4-34.23.1  
sssd-tools-1.13.4-34.23.1  
libipa\_hbac0-debuginfo-1.13.4-34.23.1  
sssd-ldap-1.13.4-34.23.1  
libipa\_hbac0-1.13.4-34.23.1  
libsss\_idmap0-1.13.4-34.23.1  
sssd-ad-1.13.4-34.23.1  
libsss\_nss\_idmap0-1.13.4-34.23.1  
sssd-krb5-common-debuginfo-1.13.4-34.23.1  
python-sssd-config-debuginfo-1.13.4-34.23.1  
sssd-tools-debuginfo-1.13.4-34.23.1  
sssd-debuginfo-32bit-1.13.4-34.23.1  
sssd-debugsource-1.13.4-34.23.1  
sssd-proxy-debuginfo-1.13.4-34.23.1  
libsss\_nss\_idmap0-debuginfo-1.13.4-34.23.1  
sssd-krb5-common-1.13.4-34.23.1  
sssd-ipa-1.13.4-34.23.1  
sssd-krb5-debuginfo-1.13.4-34.23.1  
sssd-ad-debuginfo-1.13.4-34.23.1  
sssd-proxy-1.13.4-34.23.1  
sssd-1.13.4-34.23.1  
libsss\_sudo-1.13.4-34.23.1  
sssd-32bit-1.13.4-34.23.1  
libsss\_idmap0-debuginfo-1.13.4-34.23.1  
sssd-debuginfo-1.13.4-34.23.1  
sssd-krb5-1.13.4-34.23.1  
sssd-ipa-debuginfo-1.13.4-34.23.1

## 171061 - Amazon Linux AMI ALAS-2019-1147 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19518, CVE-2018-19935

### Description

The scan detected that the host is missing the following update:  
ALAS-2019-1147

### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2019-1147.html>

## Amazon Linux AMI

x86\_64

php71-pdo-7.1.25-1.35.amzn1  
php70-mbstring-7.0.33-1.32.amzn1  
php56-mbstring-5.6.39-1.141.amzn1  
php71-pdo-dblib-7.1.25-1.35.amzn1  
php72-snmp-7.2.13-1.7.amzn1  
php71-debuginfo-7.1.25-1.35.amzn1  
php56-debuginfo-5.6.39-1.141.amzn1  
php71-7.1.25-1.35.amzn1  
php71-xmlrpc-7.1.25-1.35.amzn1  
php72-opcache-7.2.13-1.7.amzn1  
php56-intl-5.6.39-1.141.amzn1  
php56-bcmath-5.6.39-1.141.amzn1  
php71-pgsql-7.1.25-1.35.amzn1  
php70-bcmath-7.0.33-1.32.amzn1  
php56-gd-5.6.39-1.141.amzn1  
php71-dba-7.1.25-1.35.amzn1  
php72-enchanted-7.2.13-1.7.amzn1  
php56-embedded-5.6.39-1.141.amzn1  
php70-imap-7.0.33-1.32.amzn1  
php70-pdo-dblib-7.0.33-1.32.amzn1  
php70-common-7.0.33-1.32.amzn1  
php72-xml-7.2.13-1.7.amzn1  
php72-imap-7.2.13-1.7.amzn1  
php71-opcache-7.1.25-1.35.amzn1  
php71-devel-7.1.25-1.35.amzn1  
php71-dbg-7.1.25-1.35.amzn1  
php56-5.6.39-1.141.amzn1  
php71-common-7.1.25-1.35.amzn1  
php71-fpm-7.1.25-1.35.amzn1  
php70-soap-7.0.33-1.32.amzn1  
php71-snmp-7.1.25-1.35.amzn1  
php70-mysqlnd-7.0.33-1.32.amzn1  
php72-cli-7.2.13-1.7.amzn1  
php72-pspell-7.2.13-1.7.amzn1  
php56-pdo-5.6.39-1.141.amzn1  
php70-embedded-7.0.33-1.32.amzn1  
php71-enchanted-7.1.25-1.35.amzn1  
php70-zip-7.0.33-1.32.amzn1  
php71-soap-7.1.25-1.35.amzn1  
php70-process-7.0.33-1.32.amzn1  
php71-json-7.1.25-1.35.amzn1  
php56-recode-5.6.39-1.141.amzn1  
php72-recode-7.2.13-1.7.amzn1  
php70-pdo-7.0.33-1.32.amzn1  
php70-snmp-7.0.33-1.32.amzn1  
php70-mcrypt-7.0.33-1.32.amzn1  
php71-recode-7.1.25-1.35.amzn1  
php70-xmlrpc-7.0.33-1.32.amzn1  
php70-pspell-7.0.33-1.32.amzn1  
php72-embedded-7.2.13-1.7.amzn1  
php72-pdo-7.2.13-1.7.amzn1  
php72-debuginfo-7.2.13-1.7.amzn1  
php70-odbc-7.0.33-1.32.amzn1  
php71-gd-7.1.25-1.35.amzn1

php72-soap-7.2.13-1.7.amzn1  
php70- enchant-7.0.33-1.32.amzn1  
php56-process-5.6.39-1.141.amzn1  
php72-json-7.2.13-1.7.amzn1  
php72-dbg-7.2.13-1.7.amzn1  
php56-gmp-5.6.39-1.141.amzn1  
php56-mcrypt-5.6.39-1.141.amzn1  
php71-mbstring-7.1.25-1.35.amzn1  
php70-fpm-7.0.33-1.32.amzn1  
php71-bcmath-7.1.25-1.35.amzn1  
php72-xmlrpc-7.2.13-1.7.amzn1  
php70-cli-7.0.33-1.32.amzn1  
php70-gmp-7.0.33-1.32.amzn1  
php72-gd-7.2.13-1.7.amzn1  
php72-fpm-7.2.13-1.7.amzn1  
php71-mysqlnd-7.1.25-1.35.amzn1  
php56-xmlrpc-5.6.39-1.141.amzn1  
php56-dbg-5.6.39-1.141.amzn1  
php70-intl-7.0.33-1.32.amzn1  
php70-xml-7.0.33-1.32.amzn1  
php71-xml-7.1.25-1.35.amzn1  
php56-cli-5.6.39-1.141.amzn1  
php56- enchant-5.6.39-1.141.amzn1  
php72-7.2.13-1.7.amzn1  
php70-dbg-7.0.33-1.32.amzn1  
php71- imap-7.1.25-1.35.amzn1  
php71-embedded-7.1.25-1.35.amzn1  
php72-mysqlnd-7.2.13-1.7.amzn1  
php72-bcmath-7.2.13-1.7.amzn1  
php71-gmp-7.1.25-1.35.amzn1  
php71-tidy-7.1.25-1.35.amzn1  
php56-pspell-5.6.39-1.141.amzn1  
php70-7.0.33-1.32.amzn1  
php56-tidy-5.6.39-1.141.amzn1  
php56-dba-5.6.39-1.141.amzn1  
php72-pgsql-7.2.13-1.7.amzn1  
php71-pspell-7.1.25-1.35.amzn1  
php72-process-7.2.13-1.7.amzn1  
php72-ldap-7.2.13-1.7.amzn1  
php72-pdo-dblib-7.2.13-1.7.amzn1  
php70-devel-7.0.33-1.32.amzn1  
php72-gmp-7.2.13-1.7.amzn1  
php72-odbc-7.2.13-1.7.amzn1  
php70-opcache-7.0.33-1.32.amzn1  
php70-pgsql-7.0.33-1.32.amzn1  
php56-xml-5.6.39-1.141.amzn1  
php70-ldap-7.0.33-1.32.amzn1  
php56-devel-5.6.39-1.141.amzn1  
php56-snmp-5.6.39-1.141.amzn1  
php72-devel-7.2.13-1.7.amzn1  
php71-odbc-7.1.25-1.35.amzn1  
php72-dba-7.2.13-1.7.amzn1  
php56-imap-5.6.39-1.141.amzn1  
php56-pgsql-5.6.39-1.141.amzn1  
php71-ldap-7.1.25-1.35.amzn1  
php72-intl-7.2.13-1.7.amzn1  
php72-tidy-7.2.13-1.7.amzn1  
php70-json-7.0.33-1.32.amzn1  
php71-mcrypt-7.1.25-1.35.amzn1  
php56-opcache-5.6.39-1.141.amzn1

php72-common-7.2.13-1.7.amzn1  
php70-debuginfo-7.0.33-1.32.amzn1  
php71-process-7.1.25-1.35.amzn1  
php71-intl-7.1.25-1.35.amzn1  
php70-tidy-7.0.33-1.32.amzn1  
php70-recode-7.0.33-1.32.amzn1  
php56-soap-5.6.39-1.141.amzn1  
php56-odbc-5.6.39-1.141.amzn1  
php56-common-5.6.39-1.141.amzn1  
php72-mbstring-7.2.13-1.7.amzn1  
php70-gd-7.0.33-1.32.amzn1  
php56-fpm-5.6.39-1.141.amzn1  
php56-mssql-5.6.39-1.141.amzn1  
php70-dba-7.0.33-1.32.amzn1  
php56-mysqlnd-5.6.39-1.141.amzn1  
php56-ldap-5.6.39-1.141.amzn1  
php71-cli-7.1.25-1.35.amzn1

i686

php71-pdo-7.1.25-1.35.amzn1  
php70-mbstring-7.0.33-1.32.amzn1  
php56-mbstring-5.6.39-1.141.amzn1  
php71-pdo-dblib-7.1.25-1.35.amzn1  
php72-common-7.2.13-1.7.amzn1  
php71-debuginfo-7.1.25-1.35.amzn1  
php56-debuginfo-5.6.39-1.141.amzn1  
php71-7.1.25-1.35.amzn1  
php71-gmp-7.1.25-1.35.amzn1  
php72-opcache-7.2.13-1.7.amzn1  
php56-intl-5.6.39-1.141.amzn1  
php56-bcmath-5.6.39-1.141.amzn1  
php71-pgsql-7.1.25-1.35.amzn1  
php70-bcmath-7.0.33-1.32.amzn1  
php56-gd-5.6.39-1.141.amzn1  
php71-dba-7.1.25-1.35.amzn1  
php71-xmlrpc-7.1.25-1.35.amzn1  
php56-embedded-5.6.39-1.141.amzn1  
php70-imap-7.0.33-1.32.amzn1  
php70-pdo-dblib-7.0.33-1.32.amzn1  
php70-common-7.0.33-1.32.amzn1  
php72-xml-7.2.13-1.7.amzn1  
php71-opcache-7.1.25-1.35.amzn1  
php71-devel-7.1.25-1.35.amzn1  
php71-dbg-7.1.25-1.35.amzn1  
php70-tidy-7.0.33-1.32.amzn1  
php71-common-7.1.25-1.35.amzn1  
php70-soap-7.0.33-1.32.amzn1  
php72-imap-7.2.13-1.7.amzn1  
php70-mysqlnd-7.0.33-1.32.amzn1  
php72-cli-7.2.13-1.7.amzn1  
php72-pspell-7.2.13-1.7.amzn1  
php56-pdo-5.6.39-1.141.amzn1  
php70-embedded-7.0.33-1.32.amzn1  
php72-pdo-dblib-7.2.13-1.7.amzn1  
php71-mbstring-7.1.25-1.35.amzn1  
php70-zip-7.0.33-1.32.amzn1  
php71-enchanted-7.1.25-1.35.amzn1  
php71-soap-7.1.25-1.35.amzn1  
php70-process-7.0.33-1.32.amzn1  
php71-json-7.1.25-1.35.amzn1

php56-recode-5.6.39-1.141.amzn1  
php72-recode-7.2.13-1.7.amzn1  
php70-pdo-7.0.33-1.32.amzn1  
php70-snmp-7.0.33-1.32.amzn1  
php70-mcrypt-7.0.33-1.32.amzn1  
php71-recode-7.1.25-1.35.amzn1  
php70-xmlrpc-7.0.33-1.32.amzn1  
php70-pspell-7.0.33-1.32.amzn1  
php72-embedded-7.2.13-1.7.amzn1  
php72-pdo-7.2.13-1.7.amzn1  
php72-debuginfo-7.2.13-1.7.amzn1  
php70-odbc-7.0.33-1.32.amzn1  
php71-gd-7.1.25-1.35.amzn1  
php72-soap-7.2.13-1.7.amzn1  
php70-enchant-7.0.33-1.32.amzn1  
php56-process-5.6.39-1.141.amzn1  
php72-json-7.2.13-1.7.amzn1  
php72-dbg-7.2.13-1.7.amzn1  
php56-gmp-5.6.39-1.141.amzn1  
php56-mcrypt-5.6.39-1.141.amzn1  
php71-fpm-7.1.25-1.35.amzn1  
php70-fpm-7.0.33-1.32.amzn1  
php71-bcmath-7.1.25-1.35.amzn1  
php72-xmlrpc-7.2.13-1.7.amzn1  
php70-cli-7.0.33-1.32.amzn1  
php70-gmp-7.0.33-1.32.amzn1  
php72-gd-7.2.13-1.7.amzn1  
php72-fpm-7.2.13-1.7.amzn1  
php71-mysqlnd-7.1.25-1.35.amzn1  
php56-xmlrpc-5.6.39-1.141.amzn1  
php56-dbg-5.6.39-1.141.amzn1  
php70-intl-7.0.33-1.32.amzn1  
php70-xml-7.0.33-1.32.amzn1  
php71-xml-7.1.25-1.35.amzn1  
php56-cli-5.6.39-1.141.amzn1  
php56-enchant-5.6.39-1.141.amzn1  
php72-7.2.13-1.7.amzn1  
php70-dbg-7.0.33-1.32.amzn1  
php71-imap-7.1.25-1.35.amzn1  
php56-5.6.39-1.141.amzn1  
php72-mysqlnd-7.2.13-1.7.amzn1  
php71-tidy-7.1.25-1.35.amzn1  
php56-pspell-5.6.39-1.141.amzn1  
php70-7.0.33-1.32.amzn1  
php56-tidy-5.6.39-1.141.amzn1  
php72-dba-7.2.13-1.7.amzn1  
php56-dba-5.6.39-1.141.amzn1  
php72-pgsql-7.2.13-1.7.amzn1  
php71-pspell-7.1.25-1.35.amzn1  
php71-embedded-7.1.25-1.35.amzn1  
php72-process-7.2.13-1.7.amzn1  
php72-enchant-7.2.13-1.7.amzn1  
php72-gmp-7.2.13-1.7.amzn1  
php70-devel-7.0.33-1.32.amzn1

**194663 - Fedora Linux 29 FEDORA-2019-8e9789a629 Update Is Not Installed**

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

Risk Level: Medium



CVE: CVE-2018-10767

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-8e9789a629

#### 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/2019/1/?count=200&page=2>

Fedora Core 29

libgxps-0.3.1-1.fc29

### **24573 - (SB10259) McAfee Agent Privilege Escalation Vulnerability**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-6704

#### Description

A vulnerability is present in some versions of McAfee Agent.

#### Observation

McAfee Agent is client software used to communicate with McAfee ePolicy Orchestrator.

A vulnerability is present in some versions of McAfee Agent. The flaw is due to insecure handling of temporary files. Successful exploitation could allow a local attacker to perform arbitrary command execution.

### **135231 - Oracle Solaris 11.4.3.5.0 Update Is Not Installed (CVE-2018-3646)**

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

Risk Level: Medium

CVE: CVE-2018-3646

#### Description

The scan detected that the host is missing the following update:  
SRU 11.4.3.5.0

#### Observation

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

[https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&\\_adf.ctrl-state=v815z88lh\\_4&\\_afLoop=311802746081007](https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&_adf.ctrl-state=v815z88lh_4&_afLoop=311802746081007)

### **135232 - Oracle Solaris 11.4.3.5.0 Update Is Not Installed (CVE-2018-3639)**

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

Risk Level: Medium

CVE: CVE-2018-3639

### Description

The scan detected that the host is missing the following update:  
SRU 11.4.3.5.0

### Observation

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

[https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&\\_adf.ctrl-state=v815z88lh\\_4&\\_afLoop=311802746081007](https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&_adf.ctrl-state=v815z88lh_4&_afLoop=311802746081007)

## **147531 - SuSE Linux 42.3 openSUSE-SU-2019:0016-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-20467

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0016-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00015.html>

SuSE Linux 42.3

x86\_64

GraphicsMagick-debuginfo-1.3.25-123.1  
libGraphicsMagick-Q16-3-debuginfo-1.3.25-123.1  
libGraphicsMagick3-config-1.3.25-123.1  
perl-GraphicsMagick-debuginfo-1.3.25-123.1  
libGraphicsMagick-Q16-3-1.3.25-123.1  
GraphicsMagick-devel-1.3.25-123.1  
libGraphicsMagickWand-Q16-2-1.3.25-123.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-123.1  
GraphicsMagick-1.3.25-123.1  
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-123.1  
libGraphicsMagick++-Q16-12-1.3.25-123.1  
GraphicsMagick-debugsource-1.3.25-123.1  
perl-GraphicsMagick-1.3.25-123.1  
libGraphicsMagick++-devel-1.3.25-123.1

i586

GraphicsMagick-debuginfo-1.3.25-123.1  
libGraphicsMagick-Q16-3-debuginfo-1.3.25-123.1  
libGraphicsMagick3-config-1.3.25-123.1  
perl-GraphicsMagick-debuginfo-1.3.25-123.1  
libGraphicsMagick-Q16-3-1.3.25-123.1  
GraphicsMagick-devel-1.3.25-123.1  
libGraphicsMagickWand-Q16-2-1.3.25-123.1  
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-123.1  
GraphicsMagick-1.3.25-123.1  
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-123.1  
libGraphicsMagick++-Q16-12-1.3.25-123.1  
GraphicsMagick-debugsource-1.3.25-123.1  
perl-GraphicsMagick-1.3.25-123.1

## 147536 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0022-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-18718

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0022-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00031.html>

SuSE Linux 15.0

x86\_64

gthumb-debuginfo-3.6.1-lp150.3.3.1

gthumb-debugsource-3.6.1-lp150.3.3.1

gthumb-3.6.1-lp150.3.3.1

gthumb-devel-3.6.1-lp150.3.3.1

noarch

gthumb-3.6.1-bp150.2.3.1

gthumb-lang-3.6.1-lp150.3.3.1

gthumb-devel-3.6.1-bp150.2.3.1

SuSE Linux 42.3

x86\_64

gthumb-debugsource-3.4.2-7.3.1

gthumb-devel-3.4.2-7.3.1

gthumb-debuginfo-3.4.2-7.3.1

gthumb-3.4.2-7.3.1

noarch

gthumb-lang-3.4.2-7.3.1

## 147540 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0019-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11468, CVE-2018-12495

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2019:0019-1

### Observation

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

<https://lists.opensuse.org/opensuse-updates/2019-01/msg00017.html>

SuSE Linux 15.0

x86\_64

libmarkdown2-debuginfo-2.2.4-lp150.2.3.1

libmarkdown2-devel-2.2.4-lp150.2.3.1

discount-debugsource-2.2.4-lp150.2.3.1

libmarkdown2-2.2.4-lp150.2.3.1

discount-2.2.4-lp150.2.3.1

SuSE Linux 42.3

x86\_64

libmarkdown2-debuginfo-2.2.4-7.3.1

libmarkdown2-2.2.4-7.3.1

discount-debugsource-2.2.4-7.3.1

discount-2.2.4-7.3.1

libmarkdown2-devel-2.2.4-7.3.1

i586

libmarkdown2-debuginfo-2.2.4-7.3.1

libmarkdown2-2.2.4-7.3.1

discount-debugsource-2.2.4-7.3.1

discount-2.2.4-7.3.1

libmarkdown2-devel-2.2.4-7.3.1

### 163787 - Oracle Enterprise Linux ELSA-2019-4509 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10322, CVE-2018-19407, CVE-2018-19824, CVE-2018-5848, CVE-2018-7755, CVE-2018-8043

#### Description

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

ELSA-2019-4509

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2019-January/008369.html>

OEL7

x86\_64

kernel-uek-debug-4.14.35-1844.1.3.el7uek

kernel-uek-4.14.35-1844.1.3.el7uek

kernel-uek-tools-4.14.35-1844.1.3.el7uek

kernel-uek-doc-4.14.35-1844.1.3.el7uek

kernel-uek-devel-4.14.35-1844.1.3.el7uek

kernel-uek-debug-devel-4.14.35-1844.1.3.el7uek

### 171058 - Amazon Linux AMI ALAS-2019-1145 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14625, CVE-2018-20169

#### Description

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

ALAS-2019-1145

### Observation

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

<https://alas.aws.amazon.com/ALAS-2019-1145.html>

### Amazon Linux AMI

x86\_64

kernel-tools-devel-4.14.88-72.76.amzn1  
kernel-debuginfo-4.14.88-72.76.amzn1  
kernel-tools-4.14.88-72.76.amzn1  
kernel-debuginfo-common-x86\_64-4.14.88-72.76.amzn1  
perf-debuginfo-4.14.88-72.76.amzn1  
kernel-4.14.88-72.76.amzn1  
perf-4.14.88-72.76.amzn1  
kernel-devel-4.14.88-72.76.amzn1  
kernel-headers-4.14.88-72.76.amzn1  
kernel-tools-debuginfo-4.14.88-72.76.amzn1

i686

kernel-debuginfo-4.14.88-72.76.amzn1  
kernel-tools-devel-4.14.88-72.76.amzn1  
kernel-debuginfo-common-i686-4.14.88-72.76.amzn1  
kernel-tools-4.14.88-72.76.amzn1  
kernel-tools-debuginfo-4.14.88-72.76.amzn1  
perf-debuginfo-4.14.88-72.76.amzn1  
perf-4.14.88-72.76.amzn1  
kernel-devel-4.14.88-72.76.amzn1  
kernel-headers-4.14.88-72.76.amzn1  
kernel-4.14.88-72.76.amzn1

## 194659 - Fedora Linux 28 FEDORA-2019-d1b5cf0055 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0494, CVE-2018-20483

### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-d1b5cf0055

### 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/2019/1/?count=200&page=2>

Fedora Core 28

wget-1.20.1-1.fc28

## 194672 - Fedora Linux 29 FEDORA-2019-b0f7a7b74b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16862, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3701

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-b0f7a7b74b

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

kernel-headers-4.19.14-300.fc29  
kernel-tools-4.19.14-300.fc29  
kernel-4.19.14-300.fc29

### **194676 - Fedora Linux 28 FEDORA-2018-e4732930df Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-0492, CVE-2018-1000532

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-e4732930df

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

beep-1.3-26.fc28

### **194678 - Fedora Linux 28 FEDORA-2018-aadd3c2790 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-10289, CVE-2018-16647, CVE-2018-16648, CVE-2018-18662

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-aadd3c2790

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

mupdf-1.14.0-6.fc28

### 33397 - Oracle Solaris 152927-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
152927-02

#### Observation

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

<https://getupdates.oracle.com/readme/152927-02>

JavaSE 8: update 202 patch (equivalent to JDK 8u202), 64bit

SOLARIS\_10

SUNWj8dev:1.8.0,REV=2014.03.18.08.02

SUNWj8man:1.8.0,REV=2014.03.18.08.02

SUNWj8dmo:1.8.0,REV=2014.03.18.08.02

SUNWj8cfg:1.8.0,REV=2014.03.18.08.02

SUNWj8jmp:1.8.0,REV=2014.03.18.08.02

SUNWj8rt:1.8.0,REV=2014.03.18.08.02

### 33398 - Oracle Solaris 152928-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
152928-02

#### Observation

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

<https://getupdates.oracle.com/readme/152928-02>

JavaSE 8(x86): update 202 patch (equivalent to JDK 8u202), 64bit

SOLARIS\_10\_x86

SUNWj8cfg:1.8.0,REV=2014.03.18.07.33

SUNWj8man:1.8.0,REV=2014.03.18.07.33

SUNWj8dmo:1.8.0,REV=2014.03.18.07.33

SUNWj8jmp:1.8.0,REV=2014.03.18.07.33

SUNWj8rt:1.8.0,REV=2014.03.18.07.33

### 131269 - Debian Linux 9.0 DSA-4363-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3498

#### Description

The scan detected that the host is missing the following update:  
DSA-4363-1

#### Observation

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

<http://www.debian.org/security/2019/dsa-4363>

Debian 9.0

all

python-django\_1:1.10.7-2+deb9u4

### 131270 - Debian Linux 9.0 DSA-4368-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6250

#### Description

The scan detected that the host is missing the following update:  
DSA-4368-1

#### Observation

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

<http://www.debian.org/security/2019/dsa-4368>

Debian 9.0

all

libzmq5\_4.2.1-4+deb9u1

libzmq5-dbg\_4.2.1-4+deb9u1

libzmq3-dev\_4.2.1-4+deb9u1

### 131271 - Debian Linux 9.0 DSA-4365-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3461

#### Description

The scan detected that the host is missing the following update:  
DSA-4365-1



### Observation

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

<http://www.debian.org/security/2019/dsa-4365>

Debian 9.0  
all  
tmpreaper\_1.6.13+nmu1+deb9u1

### **131273 - Debian Linux 9.0 DSA-4364-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16468

### Description

The scan detected that the host is missing the following update:  
DSA-4364-1

### Observation

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

<http://www.debian.org/security/2019/dsa-4364>

Debian 9.0  
all  
ruby-loofah\_2.0.3-2+deb9u2

### **131275 - Debian Linux 9.0 DSA-4367-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

### Description

The scan detected that the host is missing the following update:  
DSA-4367-1

### Observation

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

<http://www.debian.org/security/2019/dsa-4367>

Debian 9.0  
all  
systemd\_232-25+deb9u7

### **182884 - FreeBSD py-matrix-synapse Undisclosed Vulnerability (383931ba-1818-11e9-92ea-448a5b29e8a9)**

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

Risk Level: Low

CVE: CVE-2019-5885

#### Description

The scan detected that the host is missing the following update:  
py-matrix-synapse -- undisclosed vulnerability (383931ba-1818-11e9-92ea-448a5b29e8a9)

#### Observation

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

<http://www.vuxml.org/freebsd/383931ba-1818-11e9-92ea-448a5b29e8a9.html>

Affected packages:

py27-matrix-synapse < 0.34.1.1  
py35-matrix-synapse < 0.34.1.1  
py36-matrix-synapse < 0.34.1.1  
py37-matrix-synapse < 0.34.1.1

### **186525 - Ubuntu Linux 18.04 USN-3856-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-10910

#### Description

The scan detected that the host is missing the following update:  
USN-3856-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004725.html>

Ubuntu 18.04

gnome-bluetooth\_3.28.0-2ubuntu0.1  
libgnome-bluetooth13\_3.28.0-2ubuntu0.1

### **186529 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3857-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-1000888

#### Description

The scan detected that the host is missing the following update:  
USN-3857-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004726.html>

Ubuntu 16.04

php-pear\_1.10.1+submodules+notgz-6ubuntu0.1

Ubuntu 18.10

php-pear\_1.10.5+submodules+notgz-1ubuntu1.18.10.1

Ubuntu 18.04

php-pear\_1.10.5+submodules+notgz-1ubuntu1.18.04.1

### 186534 - Ubuntu Linux 18.04, 18.10 USN-3854-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-4437

#### Description

The scan detected that the host is missing the following update:  
USN-3854-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004723.html>

Ubuntu 18.10

libwebkit2gtk-4.0-37\_2.22.5-0ubuntu0.18.10.1

libjavascriptcoregtk-4.0-18\_2.22.5-0ubuntu0.18.10.1

Ubuntu 18.04

libjavascriptcoregtk-4.0-18\_2.22.5-0ubuntu0.18.04.1

libwebkit2gtk-4.0-37\_2.22.5-0ubuntu0.18.04.1

### 186535 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3851-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3498

#### Description

The scan detected that the host is missing the following update:  
USN-3851-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004719.html>

Ubuntu 16.04

python-django\_1.8.7-1ubuntu5.7  
python3-django\_1.8.7-1ubuntu5.7

Ubuntu 18.10

python3-django\_1.11.15-1ubuntu1.1  
python-django\_1.11.15-1ubuntu1.1

Ubuntu 14.04

python-django\_1.6.11-0ubuntu1.3

Ubuntu 18.04

python3-django\_1.11.11-1ubuntu1.2  
python-django\_1.11.11-1ubuntu1.2

### **186536 - Ubuntu Linux 18.04, 18.10 USN-3853-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-1000858

#### Description

The scan detected that the host is missing the following update:  
USN-3853-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004722.html>

Ubuntu 18.10

gnupg\_2.2.8-3ubuntu1.1  
gpg-wks-client\_2.2.8-3ubuntu1.1

Ubuntu 18.04

gnupg\_2.2.4-1ubuntu1.2  
gpg-wks-client\_2.2.4-1ubuntu1.2

### **194651 - Fedora Linux 28 FEDORA-2018-36320c03cd 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-2018-36320c03cd

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

electron-cash-3.3.4-1.fc28

### **194653 - Fedora Linux 28 FEDORA-2019-944ff52ce6 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-2019-944ff52ce6

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

php-horde-Horde-Image-2.5.4-1.fc28

### **194655 - Fedora Linux 28 FEDORA-2019-1a0d4443f8 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16868

#### Description

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

FEDORA-2019-1a0d4443f8

#### 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/2019/1/?count=200&page=1>

Fedora Core 28

gnutls-3.6.5-2.fc28

### **194656 - Fedora Linux 29 FEDORA-2019-99eefddc65 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16868

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-99eefddc65

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

gnutls-3.6.5-2.fc29

### **194657 - Fedora Linux 28 FEDORA-2018-dbc80405c 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-dbc80405c

#### 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/2019/1/?count=200&page=1>

Fedora Core 28

nbdkit-1.4.4-1.fc28

### **194658 - Fedora Linux 29 FEDORA-2019-c431c60024 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-2019-c431c60024

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

electrum-3.2.4-1.fc29

### **194660 - Fedora Linux 28 FEDORA-2018-2abadd4469 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-20102, CVE-2018-20103

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-2abadd4469

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

haproxy-1.8.15-1.fc28

### **194661 - Fedora Linux 29 FEDORA-2019-31015766d1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16869

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-31015766d1

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

mingw-nettle-3.4.1-1.fc29

### **194662 - Fedora Linux 29 FEDORA-2019-1198005e1f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-1198005e1f

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

golang-1.11.4-1.fc29

#### **194665 - Fedora Linux 28 FEDORA-2019-01afc2352f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16869

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-01afc2352f

##### 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/2019/1/?count=200&page=1>

Fedora Core 28

mingw-nettle-3.4.1-1.fc28

#### **194666 - Fedora Linux 29 FEDORA-2019-e957cecffd Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-19788

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-e957cecffd

##### 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/2019/1/?count=200&page=1>

Fedora Core 29

polkit-0.115-4.2.fc29

#### **194667 - Fedora Linux 28 FEDORA-2019-24dc022a51 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-16868

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-24dc022a51



### 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/2019/1/?count=200&page=2>

Fedora Core 28

gnutls-3.6.5-1.fc28

### **194668 - Fedora Linux 29 FEDORA-2018-cb66bc33e6 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-20102, CVE-2018-20103

### Description

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

FEDORA-2018-cb66bc33e6

### 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/2019/1/?count=200&page=1>

Fedora Core 29

haproxy-1.8.15-1.fc29

### **194669 - Fedora Linux 29 FEDORA-2019-75a8da28f0 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-1000858

### Description

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

FEDORA-2019-75a8da28f0

### 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/2019/1/?count=200&page=1>

Fedora Core 29

gnupg2-2.2.12-1.fc29

### **194670 - Fedora Linux 29 FEDORA-2019-a7b53ed5a3 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2019-3498

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-a7b53ed5a3

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

python-django-2.0.10-1.fc29

### **194671 - Fedora Linux 29 FEDORA-2019-89c1abeac9 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-2019-89c1abeac9

#### 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/2019/1/?count=200&page=1>

Fedora Core 29

php-horde-Horde-Image-2.5.4-1.fc29

### **194673 - Fedora Linux 28 FEDORA-2019-ac7e19b0c8 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2018-20217

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-ac7e19b0c8

#### 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/2019/1/?count=200&page=2>

Fedora Core 28

krb5-1.16.1-24.fc28

## 194674 - Fedora Linux 28 FEDORA-2019-8f8cadd5ff 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-2019-8f8cadd5ff

### 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/2019/1/?count=200&page=1>

Fedora Core 28

thunderbird-60.4.0-1.fc28

## 194675 - Fedora Linux 28 FEDORA-2019-4dc2ccb142 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-2019-4dc2ccb142

### 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/2019/1/?count=200&page=2>

Fedora Core 28

electrum-3.2.4-1.fc28

## 194677 - Fedora Linux 28 FEDORA-2019-c424e3bb72 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-16873, CVE-2018-16874, CVE-2018-16875

### Description

The scan detected that the host is missing the following update:  
FEDORA-2019-c424e3bb72

### 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/2019/1/?count=200&page=1>

Fedora Core 28

golang-1.10.7-1.fc28

### **135230 - Oracle Solaris 11.4.3.5.0 Update Is Not Installed (CVE-2019-2437)**

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

Risk Level: Low

CVE: CVE-2019-2437

#### Description

The scan detected that the host is missing the following update:  
SRU 11.4.3.5.0

#### Observation

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

[https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&\\_adf.ctrl-state=v815z88lh\\_4&\\_afrLoop=311802746081007](https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&_adf.ctrl-state=v815z88lh_4&_afrLoop=311802746081007)

### **135233 - Oracle Solaris 11.1.19.6.0 Update Is Not Installed (CVE-2019-2543)**

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

Risk Level: Low

CVE: CVE-2019-2543

#### Description

The scan detected that the host is missing the following update:  
SRU 11.1.19.6.0

#### Observation

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

[https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&\\_adf.ctrl-state=v815z88lh\\_4&\\_afrLoop=311802746081007](https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&_adf.ctrl-state=v815z88lh_4&_afrLoop=311802746081007)

### **135234 - Oracle Solaris 11.1.19.6.0 Update Is Not Installed (CVE-2019-2544)**

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

Risk Level: Low

CVE: CVE-2019-2544

#### Description

The scan detected that the host is missing the following update:  
SRU 11.1.19.6.0

#### Observation

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

### 135235 - Oracle Solaris 11.4 Update Is Not Installed (CVE-2019-2545)

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

Risk Level: Low

CVE: CVE-2019-2545

#### Description

The scan detected that the host is missing the following update:  
SRU 11.4

#### Observation

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

[https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&\\_adf.ctrl-state=v815z88lh\\_4&\\_afLoop=311802746081007](https://support.oracle.com/epmos/faces/DocumentDisplay?id=2492126.1&_adf.ctrl-state=v815z88lh_4&_afLoop=311802746081007)

### 186530 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3850-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0495, CVE-2018-12384, CVE-2018-12404

#### Description

The scan detected that the host is missing the following update:  
USN-3850-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004720.html>

Ubuntu 16.04

libnss3\_3.28.4-0ubuntu0.16.04.4

Ubuntu 18.10

libnss3\_3.36.1-1ubuntu1.1

Ubuntu 14.04

libnss3\_3.28.4-0ubuntu0.14.04.4

Ubuntu 18.04

libnss3\_3.35-2ubuntu2.1

### 194664 - Fedora Linux 29 FEDORA-2018-92eff16e03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000532

### Description

The scan detected that the host is missing the following update:  
FEDORA-2018-92eff16e03

### 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/2019/1/?count=200&page=2>

Fedora Core 29

beep-1.3-26.fc29

## 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.

### 160465 - CentOS 6 CESA-2018-2737 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-2767

### Update Details

Risk is updated

### 163698 - Oracle Enterprise Linux ELSA-2018-2737 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-2767

### Update Details

Risk is updated

### 171022 - Amazon Linux AMI ALAS-2018-1085 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-2767

### Update Details

Risk is updated

### 175445 - Scientific Linux Security ERRATA Important: mod\_perl on SL6.x i386/x86\_64 (1809-1907)

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**186489 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3825-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**194126 - Fedora Linux 28 FEDORA-2018-0ddef94854 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**194149 - Fedora Linux 27 FEDORA-2018-a94668408d Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**194174 - Fedora Linux 29 FEDORA-2018-f6a5b71464 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**196105 - Red Hat Enterprise Linux RHSA-2018-2737 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

**196107 - Red Hat Enterprise Linux RHSA-2018-2826 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

### 196109 - Red Hat Enterprise Linux RHSA-2018-2825 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-2767

[Update Details](#)

Risk is updated

### 23714 - Google Chrome Multiple Vulnerabilities Prior To 67.0.3396.62

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

[Update Details](#)

Risk is updated

### 23715 - Google Chrome Multiple Vulnerabilities Prior To 67.0.3396.62

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

[Update Details](#)

Risk is updated

### 24632 - Microsoft Office 365 ProPlus and Office 2019 Jan 2019 Updates

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

Risk Level: High

CVE: CVE-2019-0541, CVE-2019-0559, CVE-2019-0560, CVE-2019-0561, CVE-2019-0585

[Update Details](#)

Risk is updated

### 131143 - Debian Linux 9.0 DSA-4237-1 Update Is Not Installed



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

Risk Level: High

CVE: CVE-2018-6118, CVE-2018-6120, CVE-2018-6121, CVE-2018-6122, CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147, CVE-2018-6148, CVE-2018-6149

[Update Details](#)

Risk is updated

#### 146744 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1484-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

[Update Details](#)

Risk is updated

#### 146911 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:2055-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147, CVE-2018-6148, CVE-2018-6149

[Update Details](#)

Risk is updated

#### 182700 - FreeBSD chromium Multiple Vulnerabilities (427b0f58-644c-11e8-9e1b-e8e0b747a45a)

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

[Update Details](#)

Risk is updated

#### 193826 - Fedora Linux 28 FEDORA-2018-7c80aaef26 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-

2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147, CVE-2018-6148

[Update Details](#)

Risk is updated

**193855 - Fedora Linux 27 FEDORA-2018-09b59b0227 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147, CVE-2018-6148

[Update Details](#)

Risk is updated

**196006 - Red Hat Enterprise Linux RHSA-2018-1815 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

[Update Details](#)

Risk is updated

**32160 - Oracle Solaris 136882-09 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

[Update Details](#)

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

**32163 - Oracle Solaris 136883-09 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

[Update Details](#)

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

### 33040 - Oracle Solaris 148310-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5365, CVE-2015-2662, CVE-2019-2541

#### Update Details

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

### 33060 - Oracle Solaris 148309-10 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2007-5365, CVE-2015-2662, CVE-2019-2541

#### Update Details

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

### 186468 - Ubuntu Linux 16.04 USN-3813-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000807, CVE-2018-1000808

#### Update Details

Risk is updated

### 193980 - Fedora Linux 28 FEDORA-2018-bdc5bfaedc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4180, CVE-2018-4181, CVE-2018-4182, CVE-2018-4183

#### Update Details

Risk is updated

### 194403 - Fedora Linux 29 FEDORA-2018-db05d9982f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18928

#### Update Details

Risk is updated

### 194616 - Fedora Linux 28 FEDORA-2018-1d9aa4a5fd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4180, CVE-2018-4181, CVE-2018-4182, CVE-2018-4183, CVE-2018-4700

[Update Details](#)

Risk is updated

**23599 - Google Chrome Multiple Vulnerabilities Prior To 66.0.3359.170**

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

Risk Level: Medium

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

[Update Details](#)

Risk is updated

**23600 - Google Chrome Multiple Vulnerabilities Prior To 66.0.3359.170**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

[Update Details](#)

Risk is updated

**23883 - (HT208933) Apple iTunes Vulnerabilities Prior To 12.8**

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

Risk Level: Medium

CVE: CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-4293

[Update Details](#)

Risk is updated

**23884 - (HT208934) Apple Safari Vulnerabilities Prior To 11.1.2**

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

Risk Level: Medium

CVE: CVE-2018-4260, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4274, CVE-2018-4278, CVE-2018-4279, CVE-2018-4284

[Update Details](#)

Risk is updated

**23889 - (HT208932) Apple iCloud Vulnerabilities Prior To 7.6**

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

Risk Level: Medium

CVE: CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-4293

[Update Details](#)

Risk is updated

**23893 - (HT208938) Apple iOS Multiple Vulnerabilities Prior To 11.4.1**

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-2018-4248, CVE-2018-4260, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4274, CVE-2018-4275, CVE-2018-4277, CVE-2018-4278, CVE-2018-4280, CVE-2018-4282, CVE-2018-4284, CVE-2018-4290, CVE-2018-4293

[Update Details](#)

Risk is updated

**24173 - Google Chrome Multiple Vulnerabilities Prior To 69.0.3497.81**

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

Risk Level: Medium

CVE: CVE-2018-16065, CVE-2018-16066, CVE-2018-16067, CVE-2018-16068, CVE-2018-16069, CVE-2018-16070, CVE-2018-16071, CVE-2018-16072, CVE-2018-16073, CVE-2018-16074, CVE-2018-16075, CVE-2018-16076, CVE-2018-16077, CVE-2018-16078, CVE-2018-16079, CVE-2018-16080, CVE-2018-16081, CVE-2018-16082, CVE-2018-16083, CVE-2018-16084, CVE-2018-16085, CVE-2018-16086, CVE-2018-16087, CVE-2018-16088

[Update Details](#)

Risk is updated

**24174 - Google Chrome Multiple Vulnerabilities Prior To 69.0.3497.81**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-16065, CVE-2018-16066, CVE-2018-16067, CVE-2018-16068, CVE-2018-16069, CVE-2018-16070, CVE-2018-16071, CVE-2018-16072, CVE-2018-16073, CVE-2018-16074, CVE-2018-16075, CVE-2018-16076, CVE-2018-16077, CVE-2018-16078, CVE-2018-16079, CVE-2018-16080, CVE-2018-16081, CVE-2018-16082, CVE-2018-16083, CVE-2018-16084, CVE-2018-16085, CVE-2018-16086, CVE-2018-16087, CVE-2018-16088

[Update Details](#)

Risk is updated

**31558 - Oracle Solaris 119783-41 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2008-1447, CVE-2009-0696, CVE-2010-3613, CVE-2010-3614, CVE-2011-1910, CVE-2011-2464, CVE-2011-4313, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2013-0415, CVE-2014-0591

[Update Details](#)

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

**31564 - Oracle Solaris 119784-41 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2008-1447, CVE-2009-0696, CVE-2010-3613, CVE-2010-3614, CVE-2011-1910, CVE-2011-2464, CVE-2011-4313, CVE-2012-1667, CVE-2012-3817, CVE-2012-4244, CVE-2012-5166, CVE-2013-0415, CVE-2014-0591

Update Details

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

**33145 - Oracle Solaris 150401-64 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5544, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-1171, CVE-2018-2710, CVE-2018-2717, CVE-2018-2764, CVE-2018-2903, CVE-2019-2544

Update Details

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

**131129 - Debian Linux 8.0, 9.0 DSA-4220-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6126

Update Details

Risk is updated

**141972 - Red Hat Enterprise Linux RHSA-2018-1446 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

Update Details

Risk is updated

**146672 - SuSE Linux 42.3 openSUSE-SU-2018:1275-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

Update Details

Risk is updated

**146784 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1616-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6126

[Update Details](#)

Risk is updated

**146822 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1783-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6126

[Update Details](#)

Risk is updated

**146841 - SuSE SLES 11 SP4 SUSE-SU-2018:1820-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6126

[Update Details](#)

Risk is updated

**182697 - FreeBSD chromium Multiple Vulnerabilities (e457978b-5484-11e8-9b85-54ee754af08e)**

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

Risk Level: Medium

CVE: CVE-2018-6120, CVE-2018-6121, CVE-2018-6122

[Update Details](#)

Risk is updated

**186248 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3682-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-6126

[Update Details](#)

Risk is updated

**186415 - Ubuntu Linux 18.04 USN-3781-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-4191, CVE-2018-4197, CVE-2018-4207, CVE-2018-4208, CVE-2018-4209, CVE-2018-4210, CVE-2018-4212, CVE-2018-4213, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4311, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4358, CVE-2018-4359, CVE-2018-4361

[Update Details](#)

Risk is updated

### 194196 - Fedora Linux 28 FEDORA-2018-13d8c35127 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16065, CVE-2018-16066, CVE-2018-16067, CVE-2018-16068, CVE-2018-16069, CVE-2018-16070, CVE-2018-16071, CVE-2018-16072, CVE-2018-16073, CVE-2018-16074, CVE-2018-16075, CVE-2018-16076, CVE-2018-16077, CVE-2018-16078, CVE-2018-16079, CVE-2018-16080, CVE-2018-16081, CVE-2018-16082, CVE-2018-16083, CVE-2018-16084, CVE-2018-16085, CVE-2018-16086, CVE-2018-16087, CVE-2018-16088

[Update Details](#)

Risk is updated

### 196091 - Red Hat Enterprise Linux RHSA-2018-2666 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16065, CVE-2018-16066, CVE-2018-16067, CVE-2018-16068, CVE-2018-16069, CVE-2018-16070, CVE-2018-16071, CVE-2018-16073, CVE-2018-16074, CVE-2018-16075, CVE-2018-16076, CVE-2018-16077, CVE-2018-16078, CVE-2018-16079, CVE-2018-16080, CVE-2018-16081, CVE-2018-16082, CVE-2018-16083, CVE-2018-16084, CVE-2018-16085, CVE-2018-16086, CVE-2018-16087, CVE-2018-16088

[Update Details](#)

Risk is updated

### 194615 - Fedora Linux 29 FEDORA-2018-af82e7c863 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16876

[Update Details](#)

Risk is updated

### 33162 - Oracle Solaris 150400-64 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122, CVE-2018-1171, CVE-2018-2710, CVE-2018-2717, CVE-2018-2764, CVE-2018-2903, CVE-2019-2544, CVE-2019-2545

[Update Details](#)

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

### 33291 - Oracle Solaris 150120-06 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-6481, CVE-2019-2543



Update Details

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

**33294 - Oracle Solaris 150119-06 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2014-6481, CVE-2019-2543

Update Details

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

**131267 - Debian Linux 9.0 DSA-4361-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-20430, CVE-2018-20431

Update Details

Risk is updated

**186462 - Ubuntu Linux 14.04 USN-3814-2 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-18584, CVE-2018-18585

Update Details

Risk is updated

**186471 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3814-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2018-18584, CVE-2018-18585

Update Details

Risk is updated

**192563 - Fedora Linux 26 FEDORA-2017-48f0384090 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2017-100212

Update Details

Risk is updated

### 33307 - Oracle Solaris 151934-06 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 33393 - Oracle Solaris 152925-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 33394 - Oracle Solaris 152923-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 33395 - Oracle Solaris 152926-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 33396 - Oracle Solaris 152924-11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 14345 - Microsoft Outlook Obsolete Version Detection

Category: Windows Host Assessment -> EOL and Obsolete Software  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Update Details

FASLScript is updated

### 14434 - IBM Websphere Application Server Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Update Details

FASLScript is updated

### 14438 - Red Hat Enterprise Linux Obsolete Version Detection

Category: SSH Module -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Update Details

FASLScript is updated

### 70025 - epo.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### Update Details

FASLScript is updated

## DELETED CHECKS

### 33349 - Oracle Solaris 152101-91 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### 33350 - Oracle Solaris 152100-91 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

## ADDITIONAL NOTES

- **33349** - was flagged as obsolete by the vendor.
- **33350** - was flagged as obsolete by the vendor.

## HOW TO UPDATE

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

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

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

## MCAFFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

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

Copyright 2019 McAfee, Inc.

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