

## 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

#### 20607 - (HT207170) Apple macOS Multiple Vulnerabilities Prior To 10.12

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

Risk Level: High

CVE: CVE-2016-0755, CVE-2016-4658, CVE-2016-4694, CVE-2016-4696, CVE-2016-4697, CVE-2016-4698, CVE-2016-4699, CVE-2016-4700, CVE-2016-4701, CVE-2016-4702, CVE-2016-4703, CVE-2016-4706, CVE-2016-4707, CVE-2016-4708, CVE-2016-4709, CVE-2016-4710, CVE-2016-4711, CVE-2016-4712, CVE-2016-4713, CVE-2016-4715, CVE-2016-4716, CVE-2016-4717, CVE-2016-4718, CVE-2016-4722, CVE-2016-4723, CVE-2016-4724, CVE-2016-4725, CVE-2016-4726, CVE-2016-4727, CVE-2016-4736, CVE-2016-4738, CVE-2016-4739, CVE-2016-4742, CVE-2016-4745, CVE-2016-4748, CVE-2016-4750, CVE-2016-4752, CVE-2016-4753, CVE-2016-4755, CVE-2016-4771, CVE-2016-4772, CVE-2016-4773, CVE-2016-4774, CVE-2016-4775, CVE-2016-4776, CVE-2016-4777, CVE-2016-4778, CVE-2016-4779, CVE-2016-5131, CVE-2016-5768, CVE-2016-5769, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6174, CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297

#### Description

Multiple vulnerabilities are present in some versions of Apple Mac OS X.

#### Observation

Apple Mac OS X is the operating system developed by Apple.

Multiple vulnerabilities are present in some versions of Apple Mac OS X. The flaws are mostly due to several memory corruption issues. Successful exploitation could allow an attacker to escalate privileges, retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code.

#### 191180 - Fedora Linux 23 FEDORA-2016-58f90ae3cc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-58f90ae3cc

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

mariadb-10.0.27-1.fc23

## 20604 - (SYM16-015) Symantec Messaging Gateway Decomposer Engine Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-5309, CVE-2016-5310

### Description

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway.

### Observation

Symantec Messaging Gateway is an email security solution.

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway. The flaws lie in the decomposer engine when processing RAR container files. Successful exploitation could allow an attacker to cause a denial of service condition.

## 20605 - (SYM16-015) Symantec Messaging Gateway Decomposer Engine Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5309, CVE-2016-5310

### Description

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway.

### Observation

Symantec Messaging Gateway is an email security solution.

Multiple vulnerabilities are present in some versions of Symantec Messaging Gateway. The flaws lie in the decomposer engine when processing RAR container files. Successful exploitation could allow an attacker to cause a denial of service condition.

## 130598 - Debian Linux 8.0 DSA-3682-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

### Description

The scan detected that the host is missing the following update:  
DSA-3682-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3682>

Debian 8.0

all

libc-ares2\_1.10.0-2+deb8u1

libc-ares-dev\_1.10.0-2+deb8u1

## 130602 - Debian Linux 8.0 DSA-3680-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2775, CVE-2016-2776

#### Description

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

DSA-3680-1

#### Observation

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

For more information see:

<http://www.debian.org/security/2016/dsa-3680>

Debian 8.0

all

bind9\_1:9.9.5.dfsg-9+deb8u7

### 132282 - Oracle VM OVMSA-2016-0137 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

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

OVMSA-2016-0137

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-September/000554.html>

OVM3.2

x86\_64

bind-libs-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

### 132283 - Oracle VM OVMSA-2016-0136 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

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

OVMSA-2016-0136

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-September/000555.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-September/000553.html>

OVM3.3

x86\_64

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

OVM3.4

x86\_64

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

## 141288 - Red Hat Enterprise Linux RHSA-2016-1944 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

### Description

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

RHSA-2016-1944

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-1944.html>

RHEL5S

i386

bind-devel-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-debuginfo-9.3.6-25.P1.el5\_11.9

bind-libs-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

x86\_64

bind-devel-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-debuginfo-9.3.6-25.P1.el5\_11.9

bind-libs-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

RHEL7S

noarch

bind-license-9.9.4-29.el7\_2.4

RHEL6S

i386

bind-chroot-9.8.2-0.47.rc1.el6\_8.1

bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

x86\_64

bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

RHEL6WS

x86\_64

bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1

i386

bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1

RHEL5D

x86\_64

bind-utils-9.3.6-25.P1.el5\_11.9  
bind-libs-9.3.6-25.P1.el5\_11.9  
bind-9.3.6-25.P1.el5\_11.9  
bind-debuginfo-9.3.6-25.P1.el5\_11.9  
bind-sdb-9.3.6-25.P1.el5\_11.9

i386

bind-utils-9.3.6-25.P1.el5\_11.9  
bind-libs-9.3.6-25.P1.el5\_11.9  
bind-9.3.6-25.P1.el5\_11.9  
bind-debuginfo-9.3.6-25.P1.el5\_11.9  
bind-sdb-9.3.6-25.P1.el5\_11.9

RHEL7D

x86\_64

bind-9.9.4-29.el7\_2.4  
bind-chroot-9.9.4-29.el7\_2.4  
bind-devel-9.9.4-29.el7\_2.4  
bind-libs-9.9.4-29.el7\_2.4  
bind-lite-devel-9.9.4-29.el7\_2.4  
bind-debuginfo-9.9.4-29.el7\_2.4  
bind-libs-lite-9.9.4-29.el7\_2.4  
bind-sdb-9.9.4-29.el7\_2.4  
bind-sdb-chroot-9.9.4-29.el7\_2.4  
bind-pkcs11-libs-9.9.4-29.el7\_2.4  
bind-pkcs11-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-devel-9.9.4-29.el7\_2.4

bind-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-9.9.4-29.el7\_2.4

noarch  
bind-license-9.9.4-29.el7\_2.4

RHEL6D  
x86\_64  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

i386  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

RHEL7WS  
x86\_64  
bind-pkcs11-libs-9.9.4-29.el7\_2.4  
bind-chroot-9.9.4-29.el7\_2.4  
bind-devel-9.9.4-29.el7\_2.4  
bind-libs-9.9.4-29.el7\_2.4  
bind-lite-devel-9.9.4-29.el7\_2.4  
bind-debuginfo-9.9.4-29.el7\_2.4  
bind-libs-lite-9.9.4-29.el7\_2.4  
bind-sdb-9.9.4-29.el7\_2.4  
bind-sdb-chroot-9.9.4-29.el7\_2.4  
bind-9.9.4-29.el7\_2.4  
bind-pkcs11-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-devel-9.9.4-29.el7\_2.4  
bind-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-9.9.4-29.el7\_2.4

noarch  
bind-license-9.9.4-29.el7\_2.4

## 141289 - Red Hat Enterprise Linux RHSA-2016-1978 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000111

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-1978

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1978.html>

RHEL7S  
ppc64  
python-twisted-web-12.1.0-5.el7\_2

RHEL6S  
i386  
python-twisted-web-8.2.0-5.el6\_8

x86\_64  
python-twisted-web-8.2.0-5.el6\_8

RHEL6WS  
x86\_64  
python-twisted-web-8.2.0-5.el6\_8

i386  
python-twisted-web-8.2.0-5.el6\_8

RHEL7D  
x86\_64  
python-twisted-web-12.1.0-5.el7\_2

RHEL6D  
x86\_64  
python-twisted-web-8.2.0-5.el6\_8

i386  
python-twisted-web-8.2.0-5.el6\_8

RHEL7WS  
x86\_64  
python-twisted-web-12.1.0-5.el7\_2

## 141290 - Red Hat Enterprise Linux RHSA-2016-2006 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4470, CVE-2016-5829

### Description

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

RHSA-2016-2006

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2006.html>

RHEL6D  
i386  
kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6

python-perf-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6

noarch  
kernel-firmware-2.6.32-642.6.1.el6  
kernel-abi-whitelists-2.6.32-642.6.1.el6  
kernel-doc-2.6.32-642.6.1.el6

x86\_64  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6  
kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.6.1.el6  
python-perf-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6

## RHEL6S

i386  
kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6  
python-perf-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6

noarch  
kernel-firmware-2.6.32-642.6.1.el6  
kernel-abi-whitelists-2.6.32-642.6.1.el6  
kernel-doc-2.6.32-642.6.1.el6

x86\_64  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6  
kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.6.1.el6  
python-perf-2.6.32-642.6.1.el6



kernel-headers-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6

#### RHEL6WS

i386  
kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6

#### noarch

kernel-firmware-2.6.32-642.6.1.el6  
kernel-abi-whitelists-2.6.32-642.6.1.el6  
kernel-doc-2.6.32-642.6.1.el6

#### x86\_64

kernel-debuginfo-2.6.32-642.6.1.el6  
kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
perf-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.6.1.el6  
kernel-debug-debuginfo-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6  
python-perf-debuginfo-2.6.32-642.6.1.el6

### 141293 - Red Hat Enterprise Linux RHSA-2016-2007 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5177, CVE-2016-5178

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2007

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2007.html>

#### RHEL6S

x86\_64  
chromium-browser-debuginfo-53.0.2785.143-1.el6  
chromium-browser-53.0.2785.143-1.el6

i386

chromium-browser-debuginfo-53.0.2785.143-1.el6  
chromium-browser-53.0.2785.143-1.el6

RHEL6WS  
x86\_64

chromium-browser-debuginfo-53.0.2785.143-1.el6  
chromium-browser-53.0.2785.143-1.el6

i386

chromium-browser-debuginfo-53.0.2785.143-1.el6  
chromium-browser-53.0.2785.143-1.el6

### 141294 - Red Hat Enterprise Linux RHSA-2016-1945 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-1945

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1945.html>

RHEL5S

i386

bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-debuginfo-9.7.0-21.P2.el5\_11.7

x86\_64

bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-debuginfo-9.7.0-21.P2.el5\_11.7

### 141295 - Red Hat Enterprise Linux RHSA-2016-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5257

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-1985

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1985.html>

#### RHEL6S

i386

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

x86\_64

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

#### RHEL6WS

x86\_64

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

i386

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

#### RHEL5D

x86\_64

thunderbird-debuginfo-45.4.0-1.el5\_11

thunderbird-45.4.0-1.el5\_11

i386

thunderbird-debuginfo-45.4.0-1.el5\_11

thunderbird-45.4.0-1.el5\_11

#### RHEL7D

x86\_64

thunderbird-45.4.0-1.el7\_2

thunderbird-debuginfo-45.4.0-1.el7\_2

#### RHEL6D

x86\_64

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

i386

thunderbird-debuginfo-45.4.0-1.el6\_8

thunderbird-45.4.0-1.el6\_8

#### RHEL7WS

x86\_64

thunderbird-45.4.0-1.el7\_2

thunderbird-debuginfo-45.4.0-1.el7\_2

### 144897 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2415-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5423, CVE-2016-5424

#### Description

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

SUSE-SU-2016:2415-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-September/002300.html>

SuSE SLES 12 SP1

noarch  
postgresql94-docs-9.4.9-14.1

x86\_64  
libecpg6-debuginfo-9.4.9-14.1  
libecpg6-9.4.9-14.1  
postgresql94-libs-debugsource-9.4.9-14.1  
libpq5-32bit-9.4.9-14.1  
postgresql94-debugsource-9.4.9-14.1  
postgresql94-server-debuginfo-9.4.9-14.1  
postgresql94-server-9.4.9-14.1  
libpq5-debuginfo-32bit-9.4.9-14.1  
libpq5-9.4.9-14.1  
postgresql94-9.4.9-14.1  
libpq5-debuginfo-9.4.9-14.1  
postgresql94-contrib-9.4.9-14.1  
postgresql94-debuginfo-9.4.9-14.1  
postgresql94-contrib-debuginfo-9.4.9-14.1

SuSE SLED 12 SP1

x86\_64  
libpq5-32bit-9.4.9-14.1  
libecpg6-debuginfo-9.4.9-14.1  
libpq5-debuginfo-32bit-9.4.9-14.1  
postgresql94-debuginfo-9.4.9-14.1  
postgresql94-debugsource-9.4.9-14.1  
postgresql94-9.4.9-14.1  
libecpg6-9.4.9-14.1  
libpq5-9.4.9-14.1  
libpq5-debuginfo-9.4.9-14.1  
postgresql94-libs-debugsource-9.4.9-14.1

## 144898 - SuSE Linux 13.2 openSUSE-SU-2016:2425-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5423, CVE-2016-5424

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2425-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-09/msg00110.html>

SuSE Linux 13.2

i586

libecpg6-debuginfo-9.3.14-2.13.1

libecpg6-9.3.14-2.13.1

postgresql93-test-9.3.14-2.13.1

postgresql93-debuginfo-9.3.14-2.13.1

postgresql93-pltcl-9.3.14-2.13.1

postgresql93-plperl-9.3.14-2.13.1

libpq5-9.3.14-2.13.1

libpq5-debuginfo-9.3.14-2.13.1

postgresql93-pltcl-debuginfo-9.3.14-2.13.1

postgresql93-plperl-debuginfo-9.3.14-2.13.1

postgresql93-contrib-debuginfo-9.3.14-2.13.1

postgresql93-9.3.14-2.13.1

postgresql93-devel-9.3.14-2.13.1

postgresql93-plpython-debuginfo-9.3.14-2.13.1

postgresql93-libs-debugsource-9.3.14-2.13.1

postgresql93-contrib-9.3.14-2.13.1

postgresql93-devel-debuginfo-9.3.14-2.13.1

postgresql93-server-debuginfo-9.3.14-2.13.1

postgresql93-server-9.3.14-2.13.1

postgresql93-plpython-9.3.14-2.13.1

postgresql93-debugsource-9.3.14-2.13.1

noarch

postgresql93-docs-9.3.14-2.13.1

x86\_64

libpq5-debuginfo-32bit-9.3.14-2.13.1

libecpg6-debuginfo-9.3.14-2.13.1

libecpg6-9.3.14-2.13.1

libecpg6-32bit-9.3.14-2.13.1

postgresql93-test-9.3.14-2.13.1

postgresql93-debuginfo-9.3.14-2.13.1

postgresql93-pltcl-9.3.14-2.13.1

postgresql93-plperl-9.3.14-2.13.1

libpq5-9.3.14-2.13.1

libpq5-debuginfo-9.3.14-2.13.1

postgresql93-pltcl-debuginfo-9.3.14-2.13.1

postgresql93-plperl-debuginfo-9.3.14-2.13.1

postgresql93-contrib-debuginfo-9.3.14-2.13.1

libecpg6-debuginfo-32bit-9.3.14-2.13.1

postgresql93-9.3.14-2.13.1

postgresql93-devel-9.3.14-2.13.1

postgresql93-plpython-debuginfo-9.3.14-2.13.1

postgresql93-libs-debugsource-9.3.14-2.13.1

postgresql93-contrib-9.3.14-2.13.1

postgresql93-devel-debuginfo-9.3.14-2.13.1

postgresql93-server-debuginfo-9.3.14-2.13.1

postgresql93-server-9.3.14-2.13.1

postgresql93-plpython-9.3.14-2.13.1

postgresql93-debugsource-9.3.14-2.13.1

libpq5-32bit-9.3.14-2.13.1

**144899 - SuSE Linux 13.2 openSUSE-SU-2016:2406-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-2776

## Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2406-1

## Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-09/msg00103.html>

SuSE Linux 13.2

i586

bind-chrootenv-9.9.6P1-2.22.1

bind-utils-9.9.6P1-2.22.1

bind-debuginfo-9.9.6P1-2.22.1

bind-debugsource-9.9.6P1-2.22.1

bind-lwresd-9.9.6P1-2.22.1

bind-libs-debuginfo-9.9.6P1-2.22.1

bind-libs-9.9.6P1-2.22.1

bind-utils-debuginfo-9.9.6P1-2.22.1

bind-lwresd-debuginfo-9.9.6P1-2.22.1

bind-devel-9.9.6P1-2.22.1

bind-9.9.6P1-2.22.1

noarch

bind-doc-9.9.6P1-2.22.1

x86\_64

bind-devel-9.9.6P1-2.22.1

bind-libs-32bit-9.9.6P1-2.22.1

bind-libs-debuginfo-9.9.6P1-2.22.1

bind-chrootenv-9.9.6P1-2.22.1

bind-lwresd-debuginfo-9.9.6P1-2.22.1

bind-debugsource-9.9.6P1-2.22.1

bind-lwresd-9.9.6P1-2.22.1

bind-libs-9.9.6P1-2.22.1

bind-utils-9.9.6P1-2.22.1

bind-debuginfo-9.9.6P1-2.22.1

bind-utils-debuginfo-9.9.6P1-2.22.1

bind-libs-debuginfo-32bit-9.9.6P1-2.22.1

bind-9.9.6P1-2.22.1

## **144901 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2434-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5250, CVE-2016-5257, CVE-2016-5261, CVE-2016-5270, CVE-2016-5272, CVE-2016-5274, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5280, CVE-2016-5281, CVE-2016-5284

## Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2434-1

## Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-October/002305.html>

SuSE SLES 12 SP1

x86\_64

MozillaFirefox-45.4.0esr-81.1

MozillaFirefox-debugsource-45.4.0esr-81.1

MozillaFirefox-translations-45.4.0esr-81.1

MozillaFirefox-debuginfo-45.4.0esr-81.1

SuSE SLED 12 SP1

x86\_64

MozillaFirefox-45.4.0esr-81.1

MozillaFirefox-debugsource-45.4.0esr-81.1

MozillaFirefox-translations-45.4.0esr-81.1

MozillaFirefox-debuginfo-45.4.0esr-81.1

## 144902 - SuSE Linux 13.2 openSUSE-SU-2016:2444-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418

### Description

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

openSUSE-SU-2016:2444-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-10/msg00010.html>

SuSE Linux 13.2

i586

php5-xmlreader-debuginfo-5.6.1-78.1

php5-sqlite-5.6.1-78.1

php5-ldap-debuginfo-5.6.1-78.1

php5-firebird-debuginfo-5.6.1-78.1

php5-sockets-debuginfo-5.6.1-78.1

apache2-mod\_php5-5.6.1-78.1

php5-pcntl-debuginfo-5.6.1-78.1

php5-mysql-debuginfo-5.6.1-78.1

php5-enchanted-5.6.1-78.1

php5-wddx-5.6.1-78.1

php5-readline-5.6.1-78.1

php5-xsl-5.6.1-78.1

php5-fastcgi-debuginfo-5.6.1-78.1

php5-imap-debuginfo-5.6.1-78.1

php5-exif-5.6.1-78.1

php5-fpm-5.6.1-78.1

php5-enchanted-debuginfo-5.6.1-78.1

php5-pspell-5.6.1-78.1

php5-bcmath-5.6.1-78.1

php5-sysvsem-5.6.1-78.1

php5-gd-5.6.1-78.1

php5-openssl-5.6.1-78.1

php5-mssql-debuginfo-5.6.1-78.1

php5-iconv-5.6.1-78.1

php5-mysql-5.6.1-78.1  
php5-iconv-debuginfo-5.6.1-78.1  
php5-tokenizer-debuginfo-5.6.1-78.1  
php5-xmlreader-5.6.1-78.1  
php5-sqlite-debuginfo-5.6.1-78.1  
php5-pgsql-debuginfo-5.6.1-78.1  
php5-tidy-5.6.1-78.1  
php5-xsl-debuginfo-5.6.1-78.1  
php5-posix-debuginfo-5.6.1-78.1  
php5-bz2-5.6.1-78.1  
php5-ftp-debuginfo-5.6.1-78.1  
php5-pcntl-5.6.1-78.1  
php5-openssl-debuginfo-5.6.1-78.1  
php5-odbc-debuginfo-5.6.1-78.1  
php5-debugsource-5.6.1-78.1  
php5-intl-debuginfo-5.6.1-78.1  
php5-opcache-debuginfo-5.6.1-78.1  
php5-pdo-5.6.1-78.1  
php5-pdo-debuginfo-5.6.1-78.1  
php5-pspell-debuginfo-5.6.1-78.1  
php5-opcache-5.6.1-78.1  
php5-calendar-5.6.1-78.1  
php5-odbc-5.6.1-78.1  
php5-debuginfo-5.6.1-78.1  
php5-5.6.1-78.1  
apache2-mod\_php5-debuginfo-5.6.1-78.1  
php5-phar-debuginfo-5.6.1-78.1  
php5-gmp-debuginfo-5.6.1-78.1  
php5-suhosin-5.6.1-78.1  
php5-suhosin-debuginfo-5.6.1-78.1  
php5-dba-5.6.1-78.1  
php5-sysvsem-debuginfo-5.6.1-78.1  
php5-sysvshm-5.6.1-78.1  
php5-gettext-debuginfo-5.6.1-78.1  
php5-mcrypt-debuginfo-5.6.1-78.1  
php5-fileinfo-debuginfo-5.6.1-78.1  
php5-fastcgi-5.6.1-78.1  
php5-mbstring-debuginfo-5.6.1-78.1  
php5-calendar-debuginfo-5.6.1-78.1  
php5-firebird-5.6.1-78.1  
php5-tokenizer-5.6.1-78.1  
php5-soap-5.6.1-78.1  
php5-ctype-5.6.1-78.1  
php5-ldap-5.6.1-78.1  
php5-mbstring-5.6.1-78.1  
php5-dom-debuginfo-5.6.1-78.1  
php5-curl-5.6.1-78.1  
php5-gd-debuginfo-5.6.1-78.1  
php5-intl-5.6.1-78.1  
php5-mcrypt-5.6.1-78.1  
php5-zip-5.6.1-78.1  
php5-xmlrpc-debuginfo-5.6.1-78.1  
php5-bz2-debuginfo-5.6.1-78.1  
php5-shmop-5.6.1-78.1  
php5-gettext-5.6.1-78.1  
php5-imap-5.6.1-78.1  
php5-zlib-5.6.1-78.1  
php5-dba-debuginfo-5.6.1-78.1  
php5-sockets-5.6.1-78.1  
php5-exif-debuginfo-5.6.1-78.1



php5-json-debuginfo-5.6.1-78.1  
php5-curl-debuginfo-5.6.1-78.1  
php5-sysvmsg-debuginfo-5.6.1-78.1  
php5-posix-5.6.1-78.1  
php5-bcmath-debuginfo-5.6.1-78.1  
php5-zlib-debuginfo-5.6.1-78.1  
php5-sysvmsg-5.6.1-78.1  
php5-pgsql-5.6.1-78.1  
php5-wddx-debuginfo-5.6.1-78.1  
php5-tidy-debuginfo-5.6.1-78.1  
php5-sysvshm-debuginfo-5.6.1-78.1  
php5-xmlwriter-debuginfo-5.6.1-78.1  
php5-snmp-debuginfo-5.6.1-78.1  
php5-json-5.6.1-78.1  
php5-fpm-debuginfo-5.6.1-78.1  
php5-snmp-5.6.1-78.1  
php5-soap-debuginfo-5.6.1-78.1  
php5-ctype-debuginfo-5.6.1-78.1  
php5-readline-debuginfo-5.6.1-78.1  
php5-devel-5.6.1-78.1  
php5-mssql-5.6.1-78.1  
php5-zip-debuginfo-5.6.1-78.1  
php5-dom-5.6.1-78.1  
php5-ftp-5.6.1-78.1  
php5-fileinfo-5.6.1-78.1  
php5-shmop-debuginfo-5.6.1-78.1  
php5-phar-5.6.1-78.1  
php5-gmp-5.6.1-78.1  
php5-xmlrpc-5.6.1-78.1  
php5-xmlwriter-5.6.1-78.1

noarch

php5-pear-5.6.1-78.1

x86\_64

php5-xmlreader-debuginfo-5.6.1-78.1  
php5-sqlite-5.6.1-78.1  
php5-ldap-debuginfo-5.6.1-78.1  
php5-firebird-debuginfo-5.6.1-78.1  
php5-sockets-debuginfo-5.6.1-78.1  
apache2-mod\_php5-5.6.1-78.1  
php5-pcntl-debuginfo-5.6.1-78.1  
php5-mysql-debuginfo-5.6.1-78.1  
php5-enchanted-5.6.1-78.1  
php5-wddx-5.6.1-78.1  
php5-readline-5.6.1-78.1  
php5-xsl-5.6.1-78.1  
php5-fastcgi-debuginfo-5.6.1-78.1  
php5-imap-debuginfo-5.6.1-78.1  
php5-exif-5.6.1-78.1  
php5-fpm-5.6.1-78.1  
php5-enchanted-debuginfo-5.6.1-78.1  
php5-pspell-5.6.1-78.1  
php5-bcmath-5.6.1-78.1  
php5-sysvsem-5.6.1-78.1  
php5-gd-5.6.1-78.1  
php5-openssl-5.6.1-78.1  
php5-mssql-debuginfo-5.6.1-78.1  
php5-iconv-5.6.1-78.1  
php5-mysql-5.6.1-78.1

php5-iconv-debuginfo-5.6.1-78.1  
php5-tokenizer-debuginfo-5.6.1-78.1  
php5-xmlreader-5.6.1-78.1  
php5-sqlite-debuginfo-5.6.1-78.1  
php5-pgsql-debuginfo-5.6.1-78.1  
php5-tidy-5.6.1-78.1  
php5-xsl-debuginfo-5.6.1-78.1  
php5-posix-debuginfo-5.6.1-78.1  
php5-bz2-5.6.1-78.1  
php5-ftp-debuginfo-5.6.1-78.1  
php5-pcntl-5.6.1-78.1  
php5-openssl-debuginfo-5.6.1-78.1  
php5-odbc-debuginfo-5.6.1-78.1  
php5-debugsource-5.6.1-78.1  
php5-intl-debuginfo-5.6.1-78.1  
php5-opcache-debuginfo-5.6.1-78.1  
php5-pdo-5.6.1-78.1  
php5-pdo-debuginfo-5.6.1-78.1  
php5-pspell-debuginfo-5.6.1-78.1  
php5-opcache-5.6.1-78.1  
php5-calendar-5.6.1-78.1  
php5-odbc-5.6.1-78.1  
php5-debuginfo-5.6.1-78.1  
php5-5.6.1-78.1  
apache2-mod\_php5-debuginfo-5.6.1-78.1  
php5-phar-debuginfo-5.6.1-78.1  
php5-gmp-debuginfo-5.6.1-78.1  
php5-suhosin-5.6.1-78.1  
php5-suhosin-debuginfo-5.6.1-78.1  
php5-dba-5.6.1-78.1  
php5-sysvsem-debuginfo-5.6.1-78.1  
php5-sysvshm-5.6.1-78.1  
php5-gettext-debuginfo-5.6.1-78.1  
php5-mcrypt-debuginfo-5.6.1-78.1  
php5-fileinfo-debuginfo-5.6.1-78.1  
php5-fastcgi-5.6.1-78.1  
php5-mbstring-debuginfo-5.6.1-78.1  
php5-calendar-debuginfo-5.6.1-78.1  
php5-firebird-5.6.1-78.1  
php5-tokenizer-5.6.1-78.1  
php5-soap-5.6.1-78.1  
php5-ctype-5.6.1-78.1  
php5-ldap-5.6.1-78.1  
php5-mbstring-5.6.1-78.1  
php5-dom-debuginfo-5.6.1-78.1  
php5-curl-5.6.1-78.1  
php5-gd-debuginfo-5.6.1-78.1  
php5-intl-5.6.1-78.1  
php5-mcrypt-5.6.1-78.1  
php5-zip-5.6.1-78.1  
php5-xmlrpc-debuginfo-5.6.1-78.1  
php5-bz2-debuginfo-5.6.1-78.1  
php5-shmop-5.6.1-78.1  
php5-gettext-5.6.1-78.1  
php5-imap-5.6.1-78.1  
php5-zlib-5.6.1-78.1  
php5-dba-debuginfo-5.6.1-78.1  
php5-sockets-5.6.1-78.1  
php5-exif-debuginfo-5.6.1-78.1  
php5-json-debuginfo-5.6.1-78.1

php5-curl-debuginfo-5.6.1-78.1  
php5-sysvmsg-debuginfo-5.6.1-78.1  
php5-posix-5.6.1-78.1  
php5-bcmath-debuginfo-5.6.1-78.1  
php5-zlib-debuginfo-5.6.1-78.1  
php5-sysvmsg-5.6.1-78.1  
php5-pgsql-5.6.1-78.1  
php5-wddx-debuginfo-5.6.1-78.1  
php5-tidy-debuginfo-5.6.1-78.1  
php5-sysvshm-debuginfo-5.6.1-78.1  
php5-xmlwriter-debuginfo-5.6.1-78.1  
php5-snmp-debuginfo-5.6.1-78.1  
php5-json-5.6.1-78.1  
php5-fpm-debuginfo-5.6.1-78.1  
php5-snmp-5.6.1-78.1  
php5-soap-debuginfo-5.6.1-78.1  
php5-ctype-debuginfo-5.6.1-78.1  
php5-readline-debuginfo-5.6.1-78.1  
php5-devel-5.6.1-78.1  
php5-mssql-5.6.1-78.1  
php5-zip-debuginfo-5.6.1-78.1  
php5-dom-5.6.1-78.1  
php5-ftp-5.6.1-78.1  
php5-fileinfo-5.6.1-78.1  
php5-shmop-debuginfo-5.6.1-78.1  
php5-phar-5.6.1-78.1  
php5-gmp-5.6.1-78.1  
php5-xmlrpc-5.6.1-78.1  
php5-xmlwriter-5.6.1-78.1

## 144903 - SuSE SLES 11 SP4 SUSE-SU-2016:2418-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5423, CVE-2016-5424

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2418-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-September/002302.html>

SuSE SLES 11 SP4

i586

postgresql94-docs-9.4.9-0.19.1

libecpg6-9.4.9-0.19.1

libpq5-9.4.9-0.19.1

postgresql94-server-9.4.9-0.19.1

postgresql94-9.4.9-0.19.1

postgresql94-contrib-9.4.9-0.19.1

x86\_64

postgresql94-docs-9.4.9-0.19.1

libecpg6-9.4.9-0.19.1

libpq5-9.4.9-0.19.1  
libpq5-32bit-9.4.9-0.19.1  
postgresql94-server-9.4.9-0.19.1  
postgresql94-9.4.9-0.19.1  
postgresql94-contrib-9.4.9-0.19.1

## 144904 - SuSE Linux 13.2 openSUSE-SU-2016:2443-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6323

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2443-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-10/msg00009.html>

### SuSE Linux 13.2

#### i586

glibc-debuginfo-2.19-16.28.1  
nscd-debuginfo-2.19-16.28.1  
glibc-2.19-16.28.1  
glibc-extra-debuginfo-2.19-16.28.1  
glibc-devel-debuginfo-2.19-16.28.1  
glibc-devel-2.19-16.28.1  
glibc-obsolete-debuginfo-2.19-16.28.1  
glibc-devel-static-2.19-16.28.1  
glibc-locale-2.19-16.28.1  
glibc-debugsource-2.19-16.28.1  
glibc-extra-2.19-16.28.1  
glibc-obsolete-2.19-16.28.1  
glibc-utils-2.19-16.28.1  
glibc-utils-debuginfo-2.19-16.28.1  
glibc-profile-2.19-16.28.1  
glibc-locale-debuginfo-2.19-16.28.1  
glibc-utils-debugsource-2.19-16.28.1  
nscd-2.19-16.28.1

#### i686

glibc-locale-2.19-16.28.1  
glibc-devel-2.19-16.28.1  
glibc-debugsource-2.19-16.28.1  
glibc-devel-static-2.19-16.28.1  
glibc-debuginfo-2.19-16.28.1  
glibc-devel-debuginfo-2.19-16.28.1  
glibc-2.19-16.28.1  
glibc-profile-2.19-16.28.1  
glibc-locale-debuginfo-2.19-16.28.1

#### noarch

glibc-i18ndata-2.19-16.28.1  
glibc-html-2.19-16.28.1  
glibc-info-2.19-16.28.1

x86\_64  
glibc-debuginfo-2.19-16.28.1  
glibc-utils-32bit-2.19-16.28.1  
nscd-debuginfo-2.19-16.28.1  
glibc-2.19-16.28.1  
glibc-locale-32bit-2.19-16.28.1  
glibc-extra-debuginfo-2.19-16.28.1  
glibc-debuginfo-32bit-2.19-16.28.1  
glibc-devel-debuginfo-2.19-16.28.1  
glibc-devel-static-32bit-2.19-16.28.1  
glibc-devel-2.19-16.28.1  
glibc-devel-static-2.19-16.28.1  
glibc-locale-2.19-16.28.1  
glibc-debugsource-2.19-16.28.1  
glibc-32bit-2.19-16.28.1  
glibc-extra-2.19-16.28.1  
glibc-devel-32bit-2.19-16.28.1  
glibc-profile-32bit-2.19-16.28.1  
glibc-utils-2.19-16.28.1  
glibc-utils-debuginfo-2.19-16.28.1  
glibc-profile-2.19-16.28.1  
glibc-locale-debuginfo-2.19-16.28.1  
glibc-utils-debugsource-2.19-16.28.1  
nscd-2.19-16.28.1  
glibc-locale-debuginfo-32bit-2.19-16.28.1  
glibc-utils-debuginfo-32bit-2.19-16.28.1  
glibc-devel-debuginfo-32bit-2.19-16.28.1

## 144905 - SuSE Linux 13.2 openSUSE-SU-2016:2429-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5177, CVE-2016-5178

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2429-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-10/msg00000.html>

SuSE Linux 13.2

x86\_64  
chromium-ffmpegsumo-debuginfo-53.0.2785.143-128.1  
chromedriver-53.0.2785.143-128.1  
chromium-desktop-gnome-53.0.2785.143-128.1  
chromedriver-debuginfo-53.0.2785.143-128.1  
chromium-ffmpegsumo-53.0.2785.143-128.1  
chromium-desktop-kde-53.0.2785.143-128.1  
chromium-53.0.2785.143-128.1  
chromium-debuginfo-53.0.2785.143-128.1

i586

chromium-ffmpegsumo-debuginfo-53.0.2785.143-128.1  
chromedriver-53.0.2785.143-128.1

chromium-desktop-gnome-53.0.2785.143-128.1  
chromedriver-debuginfo-53.0.2785.143-128.1  
chromium-ffmpegsumo-53.0.2785.143-128.1  
chromium-desktop-kde-53.0.2785.143-128.1  
chromium-53.0.2785.143-128.1  
chromium-debuginfo-53.0.2785.143-128.1

## 160147 - CentOS 6, 7 CESA-2016-1940 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-6304, CVE-2016-6306

### Description

The scan detected that the host is missing the following update:  
CESA-2016-1940

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-September/022096.html>  
<http://lists.centos.org/pipermail/centos-announce/2016-September/022098.html>

### CentOS 7

x86\_64  
openssl-perl-1.0.1e-51.el7\_2.7  
openssl-devel-1.0.1e-51.el7\_2.7  
openssl-libs-1.0.1e-51.el7\_2.7  
openssl-static-1.0.1e-51.el7\_2.7  
openssl-1.0.1e-51.el7\_2.7

### i686

openssl-devel-1.0.1e-51.el7\_2.7  
openssl-libs-1.0.1e-51.el7\_2.7  
openssl-static-1.0.1e-51.el7\_2.7

### CentOS 6

x86\_64  
openssl-1.0.1e-48.el6\_8.3  
openssl-perl-1.0.1e-48.el6\_8.3  
openssl-devel-1.0.1e-48.el6\_8.3  
openssl-static-1.0.1e-48.el6\_8.3

### i686

openssl-1.0.1e-48.el6\_8.3  
openssl-perl-1.0.1e-48.el6\_8.3  
openssl-devel-1.0.1e-48.el6\_8.3  
openssl-static-1.0.1e-48.el6\_8.3

## 160148 - CentOS 5, 6, 7 CESA-2016-1944 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

## Description

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

CESA-2016-1944

## Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-September/022094.html>

<http://lists.centos.org/pipermail/centos-announce/2016-September/022092.html>

<http://lists.centos.org/pipermail/centos-announce/2016-September/022097.html>

### CentOS 6

x86\_64

bind-chroot-9.8.2-0.47.rc1.el6\_8.1

bind-9.8.2-0.47.rc1.el6\_8.1

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-sdb-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

bind-devel-9.8.2-0.47.rc1.el6\_8.1

i686

bind-chroot-9.8.2-0.47.rc1.el6\_8.1

bind-9.8.2-0.47.rc1.el6\_8.1

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-sdb-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

bind-devel-9.8.2-0.47.rc1.el6\_8.1

### CentOS 7

i686

bind-libs-lite-9.9.4-29.el7\_2.4

bind-devel-9.9.4-29.el7\_2.4

bind-lite-devel-9.9.4-29.el7\_2.4

bind-libs-9.9.4-29.el7\_2.4

bind-pkcs11-libs-9.9.4-29.el7\_2.4

bind-pkcs11-devel-9.9.4-29.el7\_2.4

noarch

bind-license-9.9.4-29.el7\_2.4

x86\_64

bind-9.9.4-29.el7\_2.4

bind-chroot-9.9.4-29.el7\_2.4

bind-devel-9.9.4-29.el7\_2.4

bind-libs-9.9.4-29.el7\_2.4

bind-lite-devel-9.9.4-29.el7\_2.4

bind-libs-lite-9.9.4-29.el7\_2.4

bind-sdb-9.9.4-29.el7\_2.4

bind-sdb-chroot-9.9.4-29.el7\_2.4

bind-pkcs11-libs-9.9.4-29.el7\_2.4

bind-pkcs11-utils-9.9.4-29.el7\_2.4

bind-pkcs11-devel-9.9.4-29.el7\_2.4

bind-utils-9.9.4-29.el7\_2.4

bind-pkcs11-9.9.4-29.el7\_2.4

### CentOS 5

x86\_64

bind-devel-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9  
bind-libbind-devel-9.3.6-25.P1.el5\_11.9  
bind-9.3.6-25.P1.el5\_11.9  
bind-sdb-9.3.6-25.P1.el5\_11.9  
bind-libs-9.3.6-25.P1.el5\_11.9  
bind-chroot-9.3.6-25.P1.el5\_11.9  
bind-utils-9.3.6-25.P1.el5\_11.9

i386

bind-devel-9.3.6-25.P1.el5\_11.9  
caching-nameserver-9.3.6-25.P1.el5\_11.9  
bind-libbind-devel-9.3.6-25.P1.el5\_11.9  
bind-9.3.6-25.P1.el5\_11.9  
bind-sdb-9.3.6-25.P1.el5\_11.9  
bind-libs-9.3.6-25.P1.el5\_11.9  
bind-chroot-9.3.6-25.P1.el5\_11.9  
bind-utils-9.3.6-25.P1.el5\_11.9

### 160149 - CentOS 5 CESA-2016-1943 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3710, CVE-2016-5403

#### Description

The scan detected that the host is missing the following update:  
CESA-2016-1943

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-September/022091.html>

CentOS 5  
x86\_64  
kmod-kvm-83-276.el5.centos  
kvm-83-276.el5.centos  
kmod-kvm-debug-83-276.el5.centos  
kvm-tools-83-276.el5.centos  
kvm-qemu-img-83-276.el5.centos

### 160150 - CentOS 5 CESA-2016-1945 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

The scan detected that the host is missing the following update:  
CESA-2016-1945

#### Observation

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



<http://lists.centos.org/pipermail/centos-announce/2016-September/022093.html>

CentOS 5  
x86\_64  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7

i386  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7

### 160151 - CentOS 5, 6, 7 CESA-2016-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5257

#### Description

The scan detected that the host is missing the following update:  
CESA-2016-1985

#### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-October/022109.html>  
<http://lists.centos.org/pipermail/centos-announce/2016-October/022108.html>  
<http://lists.centos.org/pipermail/centos-announce/2016-October/022107.html>

CentOS 6  
x86\_64  
thunderbird-45.4.0-1.el6.centos

i686  
thunderbird-45.4.0-1.el6.centos

CentOS 7  
x86\_64  
thunderbird-45.4.0-1.el7.centos

CentOS 5  
x86\_64  
thunderbird-45.4.0-1.el5.centos

i386  
thunderbird-45.4.0-1.el5.centos

### 160152 - CentOS 6, 7 CESA-2016-1978 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000111

### Description

The scan detected that the host is missing the following update:  
CESA-2016-1978

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-September/022100.html>  
<http://lists.centos.org/pipermail/centos-announce/2016-September/022099.html>

CentOS 7  
x86\_64  
python-twisted-web-12.1.0-5.el7\_2

CentOS 6  
x86\_64  
python-twisted-web-8.2.0-5.el6\_8

i686  
python-twisted-web-8.2.0-5.el6\_8

## 163160 - Oracle Enterprise Linux ELSA-2016-1945 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-1945

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-September/006374.html>

OEL5  
i386  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7

x86\_64  
bind97-9.7.0-21.P2.el5\_11.7  
bind97-chroot-9.7.0-21.P2.el5\_11.7  
bind97-libs-9.7.0-21.P2.el5\_11.7  
bind97-utils-9.7.0-21.P2.el5\_11.7  
bind97-devel-9.7.0-21.P2.el5\_11.7

## 163161 - Oracle Enterprise Linux ELSA-2016-1944 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8500, CVE-2015-5477, CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776

### Description

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

ELSA-2016-1944

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-September/006373.html>

<http://oss.oracle.com/pipermail/el-errata/2016-September/006372.html>

<http://oss.oracle.com/pipermail/el-errata/2016-September/006371.html>

### OEL6

x86\_64

bind-chroot-9.8.2-0.47.rc1.el6\_8.1

bind-9.8.2-0.47.rc1.el6\_8.1

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-sdb-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

bind-devel-9.8.2-0.47.rc1.el6\_8.1

i386

bind-chroot-9.8.2-0.47.rc1.el6\_8.1

bind-9.8.2-0.47.rc1.el6\_8.1

bind-utils-9.8.2-0.47.rc1.el6\_8.1

bind-sdb-9.8.2-0.47.rc1.el6\_8.1

bind-libs-9.8.2-0.47.rc1.el6\_8.1

bind-devel-9.8.2-0.47.rc1.el6\_8.1

### OEL5

i386

bind-devel-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-libs-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

x86\_64

bind-devel-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-libs-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

### OEL7

x86\_64

bind-9.9.4-29.el7\_2.4  
bind-chroot-9.9.4-29.el7\_2.4  
bind-devel-9.9.4-29.el7\_2.4  
bind-license-9.9.4-29.el7\_2.4  
bind-libs-9.9.4-29.el7\_2.4  
bind-lite-devel-9.9.4-29.el7\_2.4  
bind-libs-lite-9.9.4-29.el7\_2.4  
bind-sdb-9.9.4-29.el7\_2.4  
bind-sdb-chroot-9.9.4-29.el7\_2.4  
bind-pkcs11-libs-9.9.4-29.el7\_2.4  
bind-pkcs11-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-devel-9.9.4-29.el7\_2.4  
bind-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-9.9.4-29.el7\_2.4

## 163162 - Oracle Enterprise Linux ELSA-2016-2006 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4470, CVE-2016-5696, CVE-2016-5829

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2006

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-October/006394.html>

### OEL6

x86\_64  
kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-abi-whitelists-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
python-perf-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
kernel-firmware-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-doc-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6

### i386

kernel-devel-2.6.32-642.6.1.el6  
kernel-2.6.32-642.6.1.el6  
kernel-abi-whitelists-2.6.32-642.6.1.el6  
kernel-headers-2.6.32-642.6.1.el6  
python-perf-2.6.32-642.6.1.el6  
kernel-debug-2.6.32-642.6.1.el6  
kernel-firmware-2.6.32-642.6.1.el6  
perf-2.6.32-642.6.1.el6  
kernel-doc-2.6.32-642.6.1.el6  
kernel-debug-devel-2.6.32-642.6.1.el6

## 163163 - Oracle Enterprise Linux ELSA-2016-1985 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5257

#### Description

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

ELSA-2016-1985

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-October/006386.html>

<http://oss.oracle.com/pipermail/el-errata/2016-October/006385.html>

OEL7

x86\_64

thunderbird-45.4.0-1.0.1.el7\_2

OEL6

x86\_64

thunderbird-45.4.0-1.0.1.el6\_8

i386

thunderbird-45.4.0-1.0.1.el6\_8

### 163164 - Oracle Enterprise Linux ELSA-2016-1978 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1000111

#### Description

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

ELSA-2016-1978

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-September/006380.html>

<http://oss.oracle.com/pipermail/el-errata/2016-September/006381.html>

OEL7

x86\_64

python-twisted-web-12.1.0-5.el7\_2

OEL6

x86\_64

python-twisted-web-8.2.0-5.el6\_8

i386

python-twisted-web-8.2.0-5.el6\_8

### 170728 - Amazon Linux AMI ALAS-2016-751 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

### Description

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

ALAS-2016-751

### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2016-751.html>

Amazon Linux AMI

x86\_64

bind-debuginfo-9.8.2-0.37.rc1.48.amzn1

bind-chroot-9.8.2-0.37.rc1.48.amzn1

bind-sdb-9.8.2-0.37.rc1.48.amzn1

bind-9.8.2-0.37.rc1.48.amzn1

bind-devel-9.8.2-0.37.rc1.48.amzn1

bind-libs-9.8.2-0.37.rc1.48.amzn1

bind-utils-9.8.2-0.37.rc1.48.amzn1

i686

bind-debuginfo-9.8.2-0.37.rc1.48.amzn1

bind-chroot-9.8.2-0.37.rc1.48.amzn1

bind-sdb-9.8.2-0.37.rc1.48.amzn1

bind-9.8.2-0.37.rc1.48.amzn1

bind-devel-9.8.2-0.37.rc1.48.amzn1

bind-libs-9.8.2-0.37.rc1.48.amzn1

bind-utils-9.8.2-0.37.rc1.48.amzn1

## 175013 - Scientific Linux Security ERRATA Important: bind97 on SL5.x i386/x86\_64 (1609-9507)

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

Risk Level: High

CVE: CVE-2016-2776

### Description

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

Security ERRATA Important: bind97 on SL5.x i386/x86\_64 (1609-9507)

### Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1609&L=scientific-linux-errata&F=&S=&P=9507>

SL5

x86\_64

bind97-libs-9.7.0-21.P2.el5\_11.7

bind97-9.7.0-21.P2.el5\_11.7

bind97-chroot-9.7.0-21.P2.el5\_11.7

bind97-devel-9.7.0-21.P2.el5\_11.7

bind97-utils-9.7.0-21.P2.el5\_11.7

bind97-debuginfo-9.7.0-21.P2.el5\_11.7

i386

bind97-libs-9.7.0-21.P2.el5\_11.7

bind97-9.7.0-21.P2.el5\_11.7

bind97-chroot-9.7.0-21.P2.el5\_11.7

bind97-devel-9.7.0-21.P2.el5\_11.7

bind97-utils-9.7.0-21.P2.el5\_11.7

bind97-debuginfo-9.7.0-21.P2.el5\_11.7

## 175014 - Scientific Linux Security ERRATA Important: bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (1609-9834)

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

Risk Level: High

CVE: CVE-2016-2776

### Description

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

Security ERRATA Important: bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (1609-9834)

### Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1609&L=scientific-linux-errata&F=&S=&P=9834>

SL5

x86\_64

bind-libs-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-devel-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-debuginfo-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

i386

bind-libs-9.3.6-25.P1.el5\_11.9

caching-nameserver-9.3.6-25.P1.el5\_11.9

bind-libbind-devel-9.3.6-25.P1.el5\_11.9

bind-9.3.6-25.P1.el5\_11.9

bind-devel-9.3.6-25.P1.el5\_11.9

bind-sdb-9.3.6-25.P1.el5\_11.9

bind-debuginfo-9.3.6-25.P1.el5\_11.9

bind-chroot-9.3.6-25.P1.el5\_11.9

bind-utils-9.3.6-25.P1.el5\_11.9

SL7

x86\_64

bind-9.9.4-29.el7\_2.4

bind-chroot-9.9.4-29.el7\_2.4

bind-devel-9.9.4-29.el7\_2.4

bind-libs-9.9.4-29.el7\_2.4

bind-lite-devel-9.9.4-29.el7\_2.4

bind-debuginfo-9.9.4-29.el7\_2.4

bind-libs-lite-9.9.4-29.el7\_2.4

bind-sdb-9.9.4-29.el7\_2.4  
bind-sdb-chroot-9.9.4-29.el7\_2.4  
bind-pkcs11-libs-9.9.4-29.el7\_2.4  
bind-pkcs11-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-devel-9.9.4-29.el7\_2.4  
bind-utils-9.9.4-29.el7\_2.4  
bind-pkcs11-9.9.4-29.el7\_2.4

noarch  
bind-license-9.9.4-29.el7\_2.4

SL6  
x86\_64  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

i386  
bind-utils-9.8.2-0.47.rc1.el6\_8.1  
bind-9.8.2-0.47.rc1.el6\_8.1  
bind-debuginfo-9.8.2-0.47.rc1.el6\_8.1  
bind-chroot-9.8.2-0.47.rc1.el6\_8.1  
bind-sdb-9.8.2-0.47.rc1.el6\_8.1  
bind-libs-9.8.2-0.47.rc1.el6\_8.1  
bind-devel-9.8.2-0.47.rc1.el6\_8.1

## 175015 - Scientific Linux Security ERRATA Important: python-twisted-web on SL6.x, SL7.x i386/x86\_64 (1609-10171)

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

Risk Level: High

CVE: CVE-2016-1000111

### Description

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

Security ERRATA Important: python-twisted-web on SL6.x, SL7.x i386/x86\_64 (1609-10171)

### Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1609&L=scientific-linux-errata&F=&S=&P=10171>

SL7  
x86\_64  
python-twisted-web-12.1.0-5.el7\_2

SL6  
x86\_64  
python-twisted-web-8.2.0-5.el6\_8

i386  
python-twisted-web-8.2.0-5.el6\_8



## 175016 - Scientific Linux Security ERRATA Important: openssl on SL6.x, SL7.x i386/x86\_64 (1609-9018)

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6304, CVE-2016-6306

### Description

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

Security ERRATA Important: openssl on SL6.x, SL7.x i386/x86\_64 (1609-9018)

### Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1609&L=scientific-linux-errata&F=&S=&P=9018>

SL7

x86\_64

openssl-libs-1.0.1e-51.el7\_2.7  
openssl-devel-1.0.1e-51.el7\_2.7  
openssl-debuginfo-1.0.1e-51.el7\_2.7  
openssl-1.0.1e-51.el7\_2.7  
openssl-static-1.0.1e-51.el7\_2.7  
openssl-perl-1.0.1e-51.el7\_2.7

SL6

x86\_64

openssl-static-1.0.1e-48.sl6\_8.3  
openssl-debuginfo-1.0.1e-48.sl6\_8.3  
openssl-devel-1.0.1e-48.sl6\_8.3  
openssl-perl-1.0.1e-48.sl6\_8.3  
openssl-1.0.1e-48.sl6\_8.3

i386

openssl-static-1.0.1e-48.sl6\_8.3  
openssl-debuginfo-1.0.1e-48.sl6\_8.3  
openssl-devel-1.0.1e-48.sl6\_8.3  
openssl-perl-1.0.1e-48.sl6\_8.3  
openssl-1.0.1e-48.sl6\_8.3

## 175017 - Scientific Linux Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (1610-78)

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

Risk Level: High

CVE: CVE-2016-5257

### Description

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

Security ERRATA Important: thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (1610-78)

### Observation

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

For more information see:

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1610&L=scientific-linux-errata&F=&S=&P=78>

SL5  
x86\_64  
thunderbird-debuginfo-45.4.0-1.el5\_11  
thunderbird-45.4.0-1.el5\_11

i386  
thunderbird-debuginfo-45.4.0-1.el5\_11  
thunderbird-45.4.0-1.el5\_11

SL7  
x86\_64  
thunderbird-45.4.0-1.el7\_2  
thunderbird-debuginfo-45.4.0-1.el7\_2

SL6  
x86\_64  
thunderbird-debuginfo-45.4.0-1.el6\_8  
thunderbird-45.4.0-1.el6\_8

i386  
thunderbird-debuginfo-45.4.0-1.el6\_8  
thunderbird-45.4.0-1.el6\_8

### 175018 - Scientific Linux Security ERRATA Important: kvm on SL5.x x86\_64 (1609-8686)

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

Risk Level: High

CVE: CVE-2016-3710, CVE-2016-5403

#### Description

The scan detected that the host is missing the following update:  
Security ERRATA Important: kvm on SL5.x x86\_64 (1609-8686)

#### Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1609&L=scientific-linux-errata&F=&S=&P=8686>

SL5  
x86\_64  
kvm-83-276.el5\_11  
kmod-kvm-debug-83-276.el5\_11  
kmod-kvm-83-276.el5\_11  
kvm-debuginfo-83-276.el5\_11  
kvm-tools-83-276.el5\_11  
kvm-qemu-img-83-276.el5\_11

### 182126 - FreeBSD BIND Remote Denial Of Service Vulnerability (c8d902b1-8550-11e6-81e7-d050996490d0)

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

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

BIND -- Remote Denial of Service vulnerability (c8d902b1-8550-11e6-81e7-d050996490d0)

### Observation

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

<http://www.vuxml.org/freebsd/c8d902b1-8550-11e6-81e7-d050996490d0.html>

Affected packages:

bind99 < 9.9.9P3

bind910 < 9.10.4P3

bind911 < 9.11.0.rc3

bind9-devel < 9.12.0.a.2016.09.10

## 185428 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3095-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7124, CVE-2016-7125, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132, CVE-2016-7133, CVE-2016-7134, CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418

### Description

The scan detected that the host is missing the following update:  
USN-3095-1

### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-October/003578.html>

Ubuntu 12.04

php5-curl\_5.3.10-1ubuntu3.25

php5-fpm\_5.3.10-1ubuntu3.25

php5-cli\_5.3.10-1ubuntu3.25

libapache2-mod-php5\_5.3.10-1ubuntu3.25

php5-cgi\_5.3.10-1ubuntu3.25

php5-mysqlnd\_5.3.10-1ubuntu3.25

php5-gd\_5.3.10-1ubuntu3.25

Ubuntu 16.04

php7.0-gd\_7.0.8-0ubuntu0.16.04.3

php7.0-cli\_7.0.8-0ubuntu0.16.04.3

php7.0-cgi\_7.0.8-0ubuntu0.16.04.3

php7.0-mysql\_7.0.8-0ubuntu0.16.04.3

php7.0-fpm\_7.0.8-0ubuntu0.16.04.3

php7.0-curl\_7.0.8-0ubuntu0.16.04.3

libapache2-mod-php7.0\_7.0.8-0ubuntu0.16.04.3

Ubuntu 14.04

php5-cli\_5.5.9+dfsg-1ubuntu4.20

php5-fpm\_5.5.9+dfsg-1ubuntu4.20

php5-cgi\_5.5.9+dfsg-1ubuntu4.20

php5-mysqlnd\_5.5.9+dfsg-1ubuntu4.20  
libapache2-mod-php5\_5.5.9+dfsg-1ubuntu4.20  
php5-gd\_5.5.9+dfsg-1ubuntu4.20  
php5-curl\_5.5.9+dfsg-1ubuntu4.20

### 191187 - Fedora Linux 24 FEDORA-2016-a555159613 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-6304, CVE-2016-6306, CVE-2016-7052

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-a555159613

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=2>

Fedora Core 24

openssl-1.0.2j-1.fc24

### 191190 - Fedora Linux 24 FEDORA-2016-cca77daf70 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-cca77daf70

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 24

bind99-9.9.9-2.P3.fc24

### 191196 - Fedora Linux 23 FEDORA-2016-14bc73b990 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7405

#### Description

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

FEDORA-2016-14bc73b990

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 23

php-adodb-5.20.6-2.fc23

### **191199 - Fedora Linux 23 FEDORA-2016-db71b72137 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7411, CVE-2016-7412, CVE-2016-7413, CVE-2016-7414, CVE-2016-7416, CVE-2016-7417, CVE-2016-7418

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-db71b72137

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 23

php-5.6.26-1.fc23

### **191201 - Fedora Linux 24 FEDORA-2016-b1b1ef703c Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7405

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-b1b1ef703c

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 24

php-adodb-5.20.6-2.fc24

### **20608 - (HT207158) Apple iTunes Multiple Vulnerabilities Prior To 12.5.1**

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-4728, CVE-2016-4758, CVE-2016-4759, CVE-2016-4760, CVE-2016-4762, CVE-2016-4763, CVE-2016-4765, CVE-2016-4766, CVE-2016-4767, CVE-2016-4768, CVE-2016-4769

#### Description

Multiple vulnerabilities are present in some versions of Apple iTunes

#### Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in WebKit. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service.

### **130597 - Debian Linux 8.0 DSA-3686-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-2836

#### Description

The scan detected that the host is missing the following update:  
DSA-3686-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3686>

Debian 8.0

all

icedove\_1:45.3.0-1~deb8u1

### **130600 - Debian Linux 8.0 DSA-3681-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-4029, CVE-2016-6634, CVE-2016-6635, CVE-2016-7168, CVE-2016-7169

#### Description

The scan detected that the host is missing the following update:  
DSA-3681-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3681>

Debian 8.0

all

wordpress\_4.1+dfsg-1+deb8u10

## 185429 - Ubuntu Linux 14.04, 16.04 USN-3092-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2119

### Description

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

USN-3092-1

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-September/003574.html>

Ubuntu 14.04

samba\_4.3.11+dfsg-0ubuntu0.14.04.1

Ubuntu 16.04

samba\_4.3.11+dfsg-0ubuntu0.16.04.1

## 20603 - (HT207171) Apple macOS Server Multiple Vulnerabilities Prior to 5.2

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

Risk Level: Medium

CVE: CVE-2016-4694, CVE-2016-4754

### Description

Multiple vulnerabilities are present in some versions of Apple macOS Server.

### Observation

Apple macOS Server provides easy to use interface to configure enterprise services for Apple devices.

Multiple vulnerabilities are present in some versions of Apple macOS Server. The flaws lie in the Apache HTTP Server and ServerDocs Server components. Successful exploitation could allow an attacker to bypass intended security restrictions or to redirect the outbound network traffic to an arbitrary proxy server.

## 20611 - (SOL21230183) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

### Description

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

### Observation

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

A special character filtering vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the ntpq component. Successful exploitation could allow an attacker to create filename with special characters when querying the NTP server which can

cause issues.

### 20612 - (SOL32790144) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7973

#### Description

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

#### Observation

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

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in network is configured for broadcast operations. Successful exploitation could allow an attacker to spoofing attack.

### 20617 - (SOL46514822) F5 BIG-IP Linux TCP Stack Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-5696

#### Description

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products.

#### Observation

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

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw in net/ipv4/tcp\_input.c file in Linux kernel before version 4.7 does not properly determine the rate of challenge ACK segments. Successful exploitation could allow an attacker to spoofing attack.

### 130601 - Debian Linux 8.0 DSA-3684-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1246

#### Description

The scan detected that the host is missing the following update:  
DSA-3684-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3684>

Debian 8.0

all

libdbd-mysql-perl\_4.028-2+deb8u2



## 144900 - SuSE SLES 11 SP4 SUSE-SU-2016:2449-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5419, CVE-2016-5420, CVE-2016-7141

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2449-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-October/002306.html>

SuSE SLES 11 SP4  
i586  
libcurl4-7.19.7-1.61.1  
curl-7.19.7-1.61.1

x86\_64  
libcurl4-7.19.7-1.61.1  
curl-7.19.7-1.61.1  
libcurl4-32bit-7.19.7-1.61.1

## 182127 - FreeBSD django CSRF Protection Bypass On A Site With Google Analytics (bb022643-84fb-11e6-a4a1-60a44ce6887b)

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

Risk Level: Medium

CVE: CVE-2016-7401

### Description

The scan detected that the host is missing the following update:  
django -- CSRF protection bypass on a site with Google Analytics (bb022643-84fb-11e6-a4a1-60a44ce6887b)

### Observation

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

<http://www.vuxml.org/freebsd/bb022643-84fb-11e6-a4a1-60a44ce6887b.html>

Affected packages:  
py-django19 < 1.9.10  
py-django18 < 1.8.15  
py-django < 1.8.15

## 185432 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3093-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1371, CVE-2016-1372, CVE-2016-1405

### Description

The scan detected that the host is missing the following update:  
USN-3093-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-September/003575.html>

Ubuntu 12.04

clamav\_0.99.2+addedllvm-0ubuntu0.12.04.1

Ubuntu 16.04

clamav\_0.99.2+dfsg-0ubuntu0.16.04.1

Ubuntu 14.04

clamav\_0.99.2+addedllvm-0ubuntu0.14.04.1

### **191182 - Fedora Linux 24 FEDORA-2016-2d9825f7c1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7445

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-2d9825f7c1

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=2>

Fedora Core 24

bind-9.10.4-2.P3.fc24

### **191183 - Fedora Linux 23 FEDORA-2016-effcc7aec Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5426, CVE-2016-5427

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-effcc7aec

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

pdns-3.4.10-1.fc23

### 191185 - Fedora Linux 24 FEDORA-2016-58a8f32c86 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7445

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-58a8f32c86

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=2>

Fedora Core 24

openjpeg2-2.1.2-1.fc24

### 191189 - Fedora Linux 24 FEDORA-2016-59fda81436 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4425

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-59fda81436

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 24

jansson-2.9-1.fc24

### 191195 - Fedora Linux 23 FEDORA-2016-cc7f19cb5b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4425

#### Description

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

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 23

jansson-2.9-1.fc23

## **20610 - (SOL01409145) F5 BIG-IP Oracle MySQL Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0641

### Description

An unspecified vulnerability present in some versions of F5 BIG-IP software components.

### Observation

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

An unspecified vulnerability present in some versions of F5 BIG-IP software components. The flaw lies in some versions of Oracle MySQL and MariaDB components. Successful exploitation could lead to unauthorized disclosure of information and disruption of service.

## **20618 - (SOL57255643) F5 BIG-IP Libssh Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0739

### Description

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products.

### Observation

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

An Information Disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in libssh library before version 0.7.3. Successful exploitation could allow an attacker to decrypt or intercept SSH sessions.

## **144896 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2453-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5350, CVE-2016-5351, CVE-2016-5352, CVE-2016-5353, CVE-2016-5354, CVE-2016-5355, CVE-2016-5356, CVE-2016-5357, CVE-2016-5358, CVE-2016-5359, CVE-2016-6504, CVE-2016-6505, CVE-2016-6506, CVE-2016-6507, CVE-2016-6508, CVE-2016-6509, CVE-2016-6510, CVE-2016-6511

### Description

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

SUSE-SU-2016:2453-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2016-October/002307.html>

SuSE SLES 12 SP1

x86\_64

wireshark-1.12.13-31.1

wireshark-debugsource-1.12.13-31.1

wireshark-debuginfo-1.12.13-31.1

SuSE SLED 12 SP1

x86\_64

wireshark-1.12.13-31.1

wireshark-debugsource-1.12.13-31.1

wireshark-debuginfo-1.12.13-31.1

## 191193 - Fedora Linux 23 FEDORA-2016-0de0e0ee0c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6161, CVE-2016-6207

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-0de0e0ee0c

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

gd-2.1.1-10.fc23

## 33355 - Oracle Solaris 147220-01 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:  
147220-01

### Observation

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

<https://getupdates.oracle.com/readme/147220-01>

SunOS 5.10(x86): libgphoto2.so.2.0.3 patch

SOLARIS\_10\_x86

SUNWgnome-camera:2.6.0,REV=10.0.3.2004.12.16.18.31

### 33356 - Oracle Solaris 147219-01 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:  
147219-01

#### Observation

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

<https://getupdates.oracle.com/readme/147219-01>

SunOS 5.10: libgphoto2.so.2.0.3 patch

SOLARIS\_10

SUNWgnome-camera:2.6.0,REV=10.0.3.2004.12.16.16.17

### 88816 - Slackware Linux 14.1, 14.2 SSA:2016-275-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
SSA:2016-275-01

#### Observation

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

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.402237>

Slackware 14.1

x86\_64

mozilla-thunderbird-45.4.0-x86\_64-1

Slackware 14.2

x86\_64

mozilla-thunderbird-45.4.0-x86\_64-1

i586

mozilla-thunderbird-45.4.0-i586-1

## 130596 - Debian Linux 8.0 DSA-3683-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5177, CVE-2016-5178

### Description

The scan detected that the host is missing the following update:  
DSA-3683-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3683>

Debian 8.0

all

chromium-dbg\_53.0.2785.143-1~deb8u1

chromium-inspector\_53.0.2785.143-1~deb8u1

chromedriver\_53.0.2785.143-1~deb8u1

chromium\_53.0.2785.143-1~deb8u1

chromium-l10n\_53.0.2785.143-1~deb8u1

## 130599 - Debian Linux 8.0 DSA-3685-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7424

### Description

The scan detected that the host is missing the following update:  
DSA-3685-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3685>

Debian 8.0

all

libavdevice55\_6:11.8-1~deb8u1

libavdevice-dev\_6:11.8-1~deb8u1

libavcodec-extra\_6:11.8-1~deb8u1

libavformat56\_6:11.8-1~deb8u1

libav-doc\_6:11.8-1~deb8u1

libavcodec-extra-56\_6:11.8-1~deb8u1

libav-dbg\_6:11.8-1~deb8u1

libavresample-dev\_6:11.8-1~deb8u1

libswscale3\_6:11.8-1~deb8u1

libswscale-dev\_6:11.8-1~deb8u1

libavformat-dev\_6:11.8-1~deb8u1

libavfilter5\_6:11.8-1~deb8u1

libavutil-dev\_6:11.8-1~deb8u1

libavresample2\_6:11.8-1~deb8u1

libav-tools\_6:11.8-1~deb8u1

libavcodec-dev\_6:11.8-1~deb8u1  
libavfilter-dev\_6:11.8-1~deb8u1  
libavcodec56\_6:11.8-1~deb8u1  
libavutil54\_6:11.8-1~deb8u1

### 141291 - Red Hat Enterprise Linux RHSA-2016-1986 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-1986

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1986.html>

RHEL4ES  
x86\_64  
redhat-release-4ES-10.13

i386  
redhat-release-4ES-10.13

RHEL4AS  
i386  
redhat-release-4AS-10.13

x86\_64  
redhat-release-4AS-10.13

### 141292 - Red Hat Enterprise Linux RHSA-2016-1990 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-1990

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-1990.html>

RHEL5D  
x86\_64  
redhat-release-5Client-5.11.0.6

i386



redhat-release-5Client-5.11.0.6  
RHEL5S  
i386  
redhat-release-5Server-5.11.0.6  
  
x86\_64  
redhat-release-5Server-5.11.0.6

### 185431 - Ubuntu Linux 16.04 USN-3094-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
USN-3094-1

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-September/003576.html>

Ubuntu 16.04

systemd\_229-4ubuntu10

### 191181 - Fedora Linux 23 FEDORA-2016-286a8ec5b0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-2016-1000232

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-286a8ec5b0

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

nodejs-tough-cookie-2.3.1-1.fc23

### 191184 - Fedora Linux 23 FEDORA-2016-aa8275e843 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-aa8275e843

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

links-2.13-1.fc23

## **191186 - Fedora Linux 24 FEDORA-2016-ea3b7e6556 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-ea3b7e6556

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 24

links-2.13-1.fc24

## **191191 - Fedora Linux 24 FEDORA-2016-c942ed0424 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7795, CVE-2016-7796

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-c942ed0424

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 24

systemd-229-15.fc24

## 191192 - Fedora Linux 23 FEDORA-2016-80f4f71eff Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7167

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-80f4f71eff

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 23

curl-7.43.0-10.fc23

## 191194 - Fedora Linux 24 FEDORA-2016-5a54fb4784 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7543

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-5a54fb4784

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 24

bash-4.3.42-7.fc24

## 191197 - Fedora Linux 23 FEDORA-2016-bc0e4e3f5a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-bc0e4e3f5a

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

community-mysql-5.6.33-1.fc23

### **191198 - Fedora Linux 24 FEDORA-2016-2d90928b5b Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-2d90928b5b

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 24

openssh-7.2p2-13.fc24

### **191200 - Fedora Linux 24 FEDORA-2016-24fa65c0ae Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-24fa65c0ae

#### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/9/?count=200&page=1>

Fedora Core 24

vfrnav-20160429-1.fc24

### **191188 - Fedora Linux 23 FEDORA-2016-4cedbd4308 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-6494

#### Description

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

### Observation

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

<https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2016/10/?count=200&page=1>

Fedora Core 23

mongodb-3.0.12-2.fc23

## ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

### 88806 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-257-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662

#### Update Details

Risk is updated

### 130583 - Debian Linux 8.0 DSA-3666-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662

#### Update Details

Risk is updated

### 182113 - FreeBSD mysql Remote Root Code Execution (856b88bf-7984-11e6-81e7-d050996490d0)

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

Risk Level: High

CVE: CVE-2016-6662

#### Update Details

Risk is updated

### 182121 - FreeBSD Remote-Code-Execution Vulnerability In Mysql And Its Variants CVE 2016-6662 (b64a7389-7c27-11e6-8aaa-5404a68ad561)

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

Risk Level: High

CVE: CVE-2016-6662

#### Update Details

Risk is updated

### 185403 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3078-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662

#### Update Details

Risk is updated

### 20482 - (MS16-110) Security Update for Microsoft Windows (3178467)

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

Risk Level: High

CVE: CVE-2016-3346, CVE-2016-3352, CVE-2016-3368, CVE-2016-3369

#### Update Details

Risk is updated

### 20490 - (MS16-108) Security Update for Microsoft Exchange Server (3185883)

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

Risk Level: High

CVE: CVE-2016-0138, CVE-2016-3378, CVE-2016-3379, CVE-2016-3574, CVE-2016-3575, CVE-2016-3576, CVE-2016-3577, CVE-2016-3578, CVE-2016-3579, CVE-2016-3580, CVE-2016-3581, CVE-2016-3582, CVE-2016-3583, CVE-2016-3590, CVE-2016-3591, CVE-2016-3592, CVE-2016-3593, CVE-2016-3594, CVE-2016-3595, CVE-2016-3596, CVE-2016-6014

#### Update Details

Risk is updated

### 130591 - Debian Linux 7.0, 8.0 DSA-3676-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1243, CVE-2016-1244

#### Update Details

Risk is updated

### 20503 - (MS16-105) Cumulative Security Update for Microsoft Edge (3183043)

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

Risk Level: High

CVE: CVE-2016-3247, CVE-2016-3291, CVE-2016-3294, CVE-2016-3295, CVE-2016-3297, CVE-2016-3325, CVE-2016-3330, CVE-2016-3350, CVE-2016-3351, CVE-2016-3370, CVE-2016-3374, CVE-2016-3377

#### Update Details

Risk is updated

### 20557 - (CTX216071) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7092, CVE-2016-7093, CVE-2016-7094, CVE-2016-7154

#### Update Details

Risk is updated

### 88809 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-271-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

#### Update Details

Risk is updated

### 130567 - Debian Linux 8.0 DSA-3653-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6354

#### Update Details

Risk is updated

### 130569 - Debian Linux 8.0 DSA-3655-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6265, CVE-2016-6525

#### Update Details

Risk is updated

### 130577 - Debian Linux 8.0 DSA-3663-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7092, CVE-2016-7094, CVE-2016-7154

#### Update Details

Risk is updated

### 130581 - Debian Linux 8.0 DSA-3664-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5426, CVE-2016-5427, CVE-2016-6172

[Update Details](#)

Risk is updated

**130584 - Debian Linux 8.0 DSA-3669-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-1240

[Update Details](#)

Risk is updated

**130585 - Debian Linux 8.0 DSA-3670-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-1240

[Update Details](#)

Risk is updated

**144877 - SuSE SLES 11 SP4 SUSE-SU-2016:2405-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-2776

[Update Details](#)

Risk is updated

**144890 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2399-1 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-2776

[Update Details](#)

Risk is updated

**181975 - FreeBSD iperf3 Buffer Overflow (d6bbf2d8-2cfc-11e6-800b-080027468580)**

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

Risk Level: High

CVE: CVE-2016-4303

[Update Details](#)

Risk is updated

**182122 - FreeBSD mozilla Multiple Vulnerabilities (2c57c47e-8bb3-4694-83c8-9fc3abad3964)**

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



Risk Level: High

CVE: CVE-2016-2827, CVE-2016-5256, CVE-2016-5257, CVE-2016-5270, CVE-2016-5271, CVE-2016-5272, CVE-2016-5273, CVE-2016-5274, CVE-2016-5275, CVE-2016-5276, CVE-2016-5277, CVE-2016-5278, CVE-2016-5279, CVE-2016-5280, CVE-2016-5281, CVE-2016-5282, CVE-2016-5283, CVE-2016-5284

[Update Details](#)

Risk is updated

#### 182125 - FreeBSD OpenSSL Multiple Vulnerabilities (43eaa656-80bc-11e6-bf52-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306, CVE-2016-6307, CVE-2016-6308

[Update Details](#)

FASLScript is updated

#### 185412 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3081-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1240

[Update Details](#)

Risk is updated

#### 185424 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3088-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2776

[Update Details](#)

Risk is updated

#### 190670 - Fedora Linux 24 FEDORA-2016-c580100c89 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6250

[Update Details](#)

Risk is updated

#### 190674 - Fedora Linux 24 FEDORA-2016-472cdec8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6250

[Update Details](#)

Risk is updated

**190692 - Fedora Linux 24 FEDORA-2016-d67864115d Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-4303

[Update Details](#)

Risk is updated

**190741 - Fedora Linux 22 FEDORA-2016-45402a6f3b Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-4303

[Update Details](#)

Risk is updated

**190766 - Fedora Linux 23 FEDORA-2016-d2ab705e4a Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-3181, CVE-2016-3182, CVE-2016-3183, CVE-2016-4796, CVE-2016-4797

[Update Details](#)

Risk is updated

**190810 - Fedora Linux 24 FEDORA-2016-8fa7ced365 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-3181, CVE-2016-3182, CVE-2016-3183, CVE-2016-4796, CVE-2016-4797

[Update Details](#)

Risk is updated

**190827 - Fedora Linux 24 FEDORA-2016-abdc548f46 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-3181, CVE-2016-3182, CVE-2016-3183, CVE-2016-4796, CVE-2016-4797

[Update Details](#)

Risk is updated

**190838 - Fedora Linux 23 FEDORA-2016-9693e82a25 Update Is Not Installed**

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

Risk Level: High  
CVE: CVE-2016-4303

[Update Details](#)

Risk is updated

**190853 - Fedora Linux 23 FEDORA-2016-14d8f9b4ed Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-8871, CVE-2016-3181, CVE-2016-3182, CVE-2016-3183, CVE-2016-4796, CVE-2016-4797

[Update Details](#)

Risk is updated

**190871 - Fedora Linux 24 FEDORA-2016-c9ad9582f7 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6354

[Update Details](#)

Risk is updated

**190971 - Fedora Linux 24 FEDORA-2016-7098bdc536 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6172

[Update Details](#)

Risk is updated

**191096 - Fedora Linux 24 FEDORA-2016-7d2c67d1f5 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7092, CVE-2016-7093, CVE-2016-7094

[Update Details](#)

Risk is updated

**191129 - Fedora Linux 25 FEDORA-2016-1d8429b89f Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7092, CVE-2016-7093, CVE-2016-7094

[Update Details](#)

Risk is updated

---

### 191148 - Fedora Linux 25 FEDORA-2016-c5ec2c17e6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7405

#### Update Details

Risk is updated

### 20576 - Google Chrome Multiple Vulnerabilities Prior To 53.0.2785.113

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

Risk Level: Medium

CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175, CVE-2016-7549

#### Update Details

Risk is updated

### 20577 - Google Chrome Multiple Vulnerabilities Prior To 53.0.2785.113

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175, CVE-2016-7549

#### Update Details

Risk is updated

### 130573 - Debian Linux 8.0 DSA-3657-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8916, CVE-2015-8917, CVE-2015-8919, CVE-2015-8920, CVE-2015-8921, CVE-2015-8922, CVE-2015-8923, CVE-2015-8924, CVE-2015-8925, CVE-2015-8926, CVE-2015-8928, CVE-2015-8930, CVE-2015-8931, CVE-2015-8932, CVE-2015-8933, CVE-2015-8934, CVE-2016-4300, CVE-2016-4302, CVE-2016-4809, CVE-2016-5844

#### Update Details

Risk is updated

### 130580 - Debian Linux 8.0 DSA-3661-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7143

#### Update Details

Risk is updated

### 132275 - Oracle VM OVMSA-2016-0104 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7092, CVE-2016-7094

[Update Details](#)

Risk is updated

**132277 - Oracle VM OVMSA-2016-0103 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7092, CVE-2016-7094

[Update Details](#)

Risk is updated

**141283 - Red Hat Enterprise Linux RHSA-2016-1905 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175, CVE-2016-5176, CVE-2016-7549

[Update Details](#)

Risk is updated CVE is updated

**144761 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1909-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8918, CVE-2015-8919, CVE-2015-8920, CVE-2015-8921, CVE-2015-8922, CVE-2015-8923, CVE-2015-8924, CVE-2015-8925, CVE-2015-8926, CVE-2015-8928, CVE-2015-8929, CVE-2015-8930, CVE-2015-8931, CVE-2015-8932, CVE-2015-8933, CVE-2015-8934, CVE-2016-4300, CVE-2016-4301, CVE-2016-4302, CVE-2016-4809

[Update Details](#)

Risk is updated

**144858 - SuSE Linux 13.2 openSUSE-SU-2016:2284-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7098

[Update Details](#)

Risk is updated

**144861 - SuSE Linux 13.2 openSUSE-SU-2016:2275-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-3623, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991

[Update Details](#)

Risk is updated

#### **144873 - SuSE Linux 13.2 openSUSE-SU-2016:2310-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175

[Update Details](#)

Risk is updated

#### **181986 - FreeBSD libarchive Multiple Vulnerabilities (4a0d9b53-395d-11e6-b3c8-14dae9d210b8)**

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

Risk Level: Medium

CVE: CVE-2015-8934, CVE-2016-4300, CVE-2016-4301, CVE-2016-4302

[Update Details](#)

Risk is updated

#### **182117 - FreeBSD chromium Multiple Vulnerabilities (653a8059-7c49-11e6-9242-3065ec8fd3ec)**

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

Risk Level: Medium

CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175

[Update Details](#)

Risk is updated

#### **185364 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-3033-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8916, CVE-2015-8917, CVE-2015-8919, CVE-2015-8920, CVE-2015-8921, CVE-2015-8922, CVE-2015-8923, CVE-2015-8924, CVE-2015-8925, CVE-2015-8926, CVE-2015-8928, CVE-2015-8930, CVE-2015-8931, CVE-2015-8932, CVE-2015-8933, CVE-2015-8934, CVE-2016-4300, CVE-2016-4302, CVE-2016-4809, CVE-2016-5844

[Update Details](#)

Risk is updated

#### **191105 - Fedora Linux 24 FEDORA-2016-27d3b7742f Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

#### **191120 - Fedora Linux 24 FEDORA-2016-2eac99579c Update Is Not Installed**

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

Risk Level: Medium  
CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

**191121 - Fedora Linux 23 FEDORA-2016-231f53426b Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

**191124 - Fedora Linux 24 FEDORA-2016-b15185b72a Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-5170, CVE-2016-5171, CVE-2016-5172, CVE-2016-5173, CVE-2016-5174, CVE-2016-5175

[Update Details](#)

Risk is updated

**191125 - Fedora Linux 25 FEDORA-2016-8ed6b7bb5e Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

**191127 - Fedora Linux 25 FEDORA-2016-dc53ceffc2 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

**191128 - Fedora Linux 23 FEDORA-2016-adb346980c Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes  
Risk Level: Medium  
CVE: CVE-2016-7163

[Update Details](#)

Risk is updated

### **88811 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-265-03 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7044, CVE-2016-7045

#### Update Details

Risk is updated

### **88813 - Slackware Linux 14.2 SSA:2016-270-01 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7052

#### Update Details

Risk is updated

### **130593 - Debian Linux 8.0 DSA-3672-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7044, CVE-2016-7045

#### Update Details

Risk is updated

### **130595 - Debian Linux 8.0 DSA-3678-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7401

#### Update Details

Risk is updated

### **141273 - Red Hat Enterprise Linux RHSA-2016-1850 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8920, CVE-2015-8921, CVE-2015-8932, CVE-2016-4809, CVE-2016-5418, CVE-2016-5844, CVE-2016-7166

#### Update Details

Risk is updated

### **144718 - SuSE Linux 13.2 openSUSE-SU-2016:1679-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-4809



[Update Details](#)

Risk is updated

**144863 - SuSE Linux 13.2 openSUSE-SU-2016:2276-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6352

[Update Details](#)

Risk is updated

**144875 - SuSE Linux 13.2 openSUSE-SU-2016:2338-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7162

[Update Details](#)

Risk is updated

**160144 - CentOS 6 CESA-2016-1850 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8920, CVE-2015-8921, CVE-2015-8932, CVE-2016-4809, CVE-2016-5418, CVE-2016-5844, CVE-2016-7166

[Update Details](#)

Risk is updated

**163150 - Oracle Enterprise Linux ELSA-2016-1850 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8920, CVE-2015-8921, CVE-2015-8932, CVE-2016-4809, CVE-2016-5418, CVE-2016-5844, CVE-2016-7166

[Update Details](#)

Risk is updated

**170725 - Amazon Linux AMI ALAS-2016-742 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7141, CVE-2016-7167

[Update Details](#)

Risk is updated

**175010 - Scientific Linux Security ERRATA Important: libarchive on SL6.x i386/x86\_64 (1609-750)**

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

Risk Level: Medium

CVE: CVE-2015-8920, CVE-2015-8921, CVE-2015-8932, CVE-2016-4809, CVE-2016-5418, CVE-2016-5844, CVE-2016-7166

[Update Details](#)

Risk is updated

#### **182123 - FreeBSD irssi Heap Corruption And Missing Boundary Checks (e78261e4-803d-11e6-a590-14dae9d210b8)**

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

Risk Level: Medium

CVE: CVE-2016-7044, CVE-2016-7045

[Update Details](#)

Risk is updated

#### **185405 - Ubuntu Linux 14.04, 16.04 USN-3074-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7162

[Update Details](#)

Risk is updated

#### **185420 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3089-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7401

[Update Details](#)

Risk is updated

#### **185421 - Ubuntu Linux 16.04 USN-3086-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7044, CVE-2016-7045

[Update Details](#)

Risk is updated

#### **191132 - Fedora Linux 25 FEDORA-2016-2939d70cf4 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6802

[Update Details](#)

Risk is updated

### 191157 - Fedora Linux 25 FEDORA-2016-0cadb1feae Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7044, CVE-2016-7045

#### Update Details

Risk is updated

### 20487 - (MS16-115) Security Update for Microsoft Windows PDF Library (3188733)

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

Risk Level: Medium

CVE: CVE-2016-3370, CVE-2016-3374

#### Update Details

Risk is updated

### 20530 - (MS16-111) Security Update for Windows Kernel (3186973)

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

Risk Level: Medium

CVE: CVE-2016-3305, CVE-2016-3306, CVE-2016-3371, CVE-2016-3372, CVE-2016-3373

#### Update Details

Risk is updated

### 20532 - Wireshark Multiple Vulnerabilities Prior To 2.0.6

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

Risk Level: Medium

CVE: CVE-2016-7175, CVE-2016-7176, CVE-2016-7177, CVE-2016-7178, CVE-2016-7179, CVE-2016-7180

#### Update Details

Risk is updated

### 130578 - Debian Linux 8.0 DSA-3662-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7142

#### Update Details

Risk is updated

### 144757 - SuSE Linux 13.2 openSUSE-SU-2016:1932-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6153

[Update Details](#)

Risk is updated

#### **144768 - SuSE Linux 13.2 openSUSE-SU-2016:1926-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6265

[Update Details](#)

Risk is updated

#### **144772 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1945-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6153

[Update Details](#)

Risk is updated

#### **144791 - SuSE SLES 11 SP4 SUSE-SU-2016:2021-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6153

[Update Details](#)

Risk is updated

#### **144840 - SuSE Linux 13.2 openSUSE-SU-2016:2203-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6905

[Update Details](#)

Risk is updated

#### **182000 - FreeBSD SQLite3 Tempdir Selection Vulnerability (546deeea-3fc6-11e6-a671-60a44ce6887b)**

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

Risk Level: Medium

CVE: CVE-2016-6153

[Update Details](#)

Risk is updated

### 190918 - Fedora Linux 24 FEDORA-2016-0138339b54 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6153

#### [Update Details](#)

Risk is updated

### 191172 - Fedora Linux 25 FEDORA-2016-9a8e2bbc04 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-6494

#### [Update Details](#)

Risk is updated

### 144830 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2189-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5746

#### [Update Details](#)

Risk is updated

### 144895 - SuSE SLES 11 SP4 SUSE-SU-2016:2353-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5746

#### [Update Details](#)

Risk is updated

### 14530 - Compaq Insight Manager Obsolete Version Detection

Category: General Vulnerability Assessment -> NonIntrusive -> EOL and Obsolete Software

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

#### [Update Details](#)

FASLScript is updated

### 70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

## Update Details

FASLScript is updated

## HOW TO UPDATE

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

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

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

## MCAFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

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

Copyright 2016 McAfee, Inc.

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