

## 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

#### 141049 - Red Hat Enterprise Linux RHSA-2015-2697 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

#### Description

The scan detected that the host is missing the following update:  
RHSA-2015-2697

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2015-2697.html>

RHEL5S  
x86\_64  
flash-plugin-11.2.202.559-1.el5

i386  
flash-plugin-11.2.202.559-1.el5

RHEL6D  
x86\_64  
flash-plugin-11.2.202.559-1.el6\_7

i386  
flash-plugin-11.2.202.559-1.el6\_7

RHEL6S  
x86\_64  
flash-plugin-11.2.202.559-1.el6\_7

i386  
flash-plugin-11.2.202.559-1.el6\_7

RHEL6WS  
x86\_64  
flash-plugin-11.2.202.559-1.el6\_7

i386  
flash-plugin-11.2.202.559-1.el6\_7

RHEL5D  
x86\_64  
flash-plugin-11.2.202.559-1.el5

i386  
flash-plugin-11.2.202.559-1.el5

## 144112 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2353-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2353-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00104.html>

SuSE Linux 13.1  
x86\_64  
MozillaFirefox-43.0-97.1  
MozillaFirefox-translations-common-43.0-97.1  
MozillaFirefox-debugsource-43.0-97.1  
MozillaFirefox-translations-other-43.0-97.1  
MozillaFirefox-devel-43.0-97.1  
MozillaFirefox-branding-upstream-43.0-97.1  
MozillaFirefox-debuginfo-43.0-97.1  
MozillaFirefox-buildsymbols-43.0-97.1

i586  
MozillaFirefox-43.0-97.1  
MozillaFirefox-translations-common-43.0-97.1  
MozillaFirefox-debugsource-43.0-97.1  
MozillaFirefox-translations-other-43.0-97.1  
MozillaFirefox-devel-43.0-97.1  
MozillaFirefox-branding-upstream-43.0-97.1  
MozillaFirefox-debuginfo-43.0-97.1  
MozillaFirefox-buildsymbols-43.0-97.1

SuSE Linux 13.2  
x86\_64  
MozillaFirefox-debuginfo-43.0-53.1  
MozillaFirefox-translations-other-43.0-53.1  
MozillaFirefox-branding-upstream-43.0-53.1  
MozillaFirefox-buildsymbols-43.0-53.1  
MozillaFirefox-debugsource-43.0-53.1  
MozillaFirefox-translations-common-43.0-53.1  
MozillaFirefox-43.0-53.1  
MozillaFirefox-devel-43.0-53.1

i586

MozillaFirefox-debuginfo-43.0-53.1  
MozillaFirefox-translations-other-43.0-53.1  
MozillaFirefox-branding-upstream-43.0-53.1  
MozillaFirefox-buildsymbols-43.0-53.1  
MozillaFirefox-debugsource-43.0-53.1  
MozillaFirefox-translations-common-43.0-53.1  
MozillaFirefox-43.0-53.1  
MozillaFirefox-devel-43.0-53.1

### 181737 - FreeBSD flash Multiple Vulnerabilities (84c7ea88-bf04-4bdc-973b-36744bf540ab)

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

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

#### Description

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

flash -- multiple vulnerabilities (84c7ea88-bf04-4bdc-973b-36744bf540ab)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/84c7ea88-bf04-4bdc-973b-36744bf540ab.html>

Affected packages:

linux-c6-flashplugin < 11.2r202.559

linux-f10-flashplugin < 11.2r202.559

linux-c6\_64-flashplugin < 11.2r202.559

### 19444 - (SOL17407) F5 BIG-IP Datastor Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-7394

#### Description

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

#### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the datastor kernel module. Successful exploitation could allow an attacker to cause a denial of service condition or elevate its privileges.

### 19478 - Opera Multiple Vulnerabilities Prior To 34

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

## Description

Multiple vulnerabilities are present in some versions of Opera.

## Observation

Opera is a popular web browser.

Multiple vulnerabilities are present in some versions of Opera. The flaws lie in Chromium/Blink used by Opera. Successful exploitation could allow an attacker to execute arbitrary code.

## 19443 - (SOL17239) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-9529

## Description

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

## Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the kernel during garbage collection of keys. Successful exploitation could allow an attacker to cause a denial of service condition.

## 130348 - Debian Linux 7.0, 8.0 DSA-3430-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035, CVE-2015-8241, CVE-2015-8317

## Description

The scan detected that the host is missing the following update:  
DSA-3430-1

## Observation

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

<http://www.debian.org/security/2015/dsa-3430>

Debian 8.0

all  
libxml2\_2.9.1+dfsg1-5+deb8u1

Debian 7.0

all  
libxml2\_2.8.0+dfsg1-7+wheezy5

## 144107 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2362-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5343

## Description

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

openSUSE-SU-2015:2362-1

## Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00110.html>

SuSE Linux 13.1

i586

subversion-server-1.8.15-2.42.1

libsvn\_auth\_gnome\_keyring-1-0-debuginfo-1.8.15-2.42.1

libsvn\_auth\_gnome\_keyring-1-0-1.8.15-2.42.1

subversion-perl-1.8.15-2.42.1

subversion-ruby-debuginfo-1.8.15-2.42.1

subversion-1.8.15-2.42.1

subversion-python-1.8.15-2.42.1

subversion-tools-1.8.15-2.42.1

subversion-ruby-1.8.15-2.42.1

libsvn\_auth\_kwallet-1-0-debuginfo-1.8.15-2.42.1

subversion-devel-1.8.15-2.42.1

subversion-perl-debuginfo-1.8.15-2.42.1

subversion-debuginfo-1.8.15-2.42.1

libsvn\_auth\_kwallet-1-0-1.8.15-2.42.1

subversion-python-debuginfo-1.8.15-2.42.1

subversion-debugsource-1.8.15-2.42.1

subversion-tools-debuginfo-1.8.15-2.42.1

subversion-server-debuginfo-1.8.15-2.42.1

noarch

subversion-bash-completion-1.8.15-2.42.1

x86\_64

subversion-server-1.8.15-2.42.1

libsvn\_auth\_gnome\_keyring-1-0-debuginfo-1.8.15-2.42.1

libsvn\_auth\_gnome\_keyring-1-0-1.8.15-2.42.1

subversion-perl-1.8.15-2.42.1

subversion-ruby-debuginfo-1.8.15-2.42.1

subversion-1.8.15-2.42.1

subversion-python-1.8.15-2.42.1

subversion-tools-1.8.15-2.42.1

subversion-ruby-1.8.15-2.42.1

libsvn\_auth\_kwallet-1-0-debuginfo-1.8.15-2.42.1

subversion-devel-1.8.15-2.42.1

subversion-perl-debuginfo-1.8.15-2.42.1

subversion-debuginfo-1.8.15-2.42.1

libsvn\_auth\_kwallet-1-0-1.8.15-2.42.1

subversion-python-debuginfo-1.8.15-2.42.1

subversion-debugsource-1.8.15-2.42.1

subversion-tools-debuginfo-1.8.15-2.42.1

subversion-server-debuginfo-1.8.15-2.42.1

SuSE Linux 13.2

i586

subversion-python-ctypes-1.8.15-2.23.1

libsvn\_auth\_kwallet-1-0-debuginfo-1.8.15-2.23.1

subversion-python-debuginfo-1.8.15-2.23.1  
libsvn\_auth\_gnome\_keyring-1-0-1.8.15-2.23.1  
subversion-1.8.15-2.23.1  
libsvn\_auth\_gnome\_keyring-1-0-debuginfo-1.8.15-2.23.1  
subversion-debugsource-1.8.15-2.23.1  
subversion-python-1.8.15-2.23.1  
subversion-tools-debuginfo-1.8.15-2.23.1  
subversion-server-debuginfo-1.8.15-2.23.1  
subversion-devel-1.8.15-2.23.1  
subversion-perl-1.8.15-2.23.1  
libsvn\_auth\_kwallet-1-0-1.8.15-2.23.1  
subversion-server-1.8.15-2.23.1  
subversion-debuginfo-1.8.15-2.23.1  
subversion-tools-1.8.15-2.23.1  
subversion-ruby-1.8.15-2.23.1  
subversion-perl-debuginfo-1.8.15-2.23.1  
subversion-ruby-debuginfo-1.8.15-2.23.1

noarch

subversion-bash-completion-1.8.15-2.23.1

x86\_64

subversion-python-ctypes-1.8.15-2.23.1  
libsvn\_auth\_kwallet-1-0-debuginfo-1.8.15-2.23.1  
subversion-python-debuginfo-1.8.15-2.23.1  
libsvn\_auth\_gnome\_keyring-1-0-1.8.15-2.23.1  
subversion-1.8.15-2.23.1  
libsvn\_auth\_gnome\_keyring-1-0-debuginfo-1.8.15-2.23.1  
subversion-debugsource-1.8.15-2.23.1  
subversion-python-1.8.15-2.23.1  
subversion-tools-debuginfo-1.8.15-2.23.1  
subversion-server-debuginfo-1.8.15-2.23.1  
subversion-devel-1.8.15-2.23.1  
subversion-perl-1.8.15-2.23.1  
libsvn\_auth\_kwallet-1-0-1.8.15-2.23.1  
subversion-server-1.8.15-2.23.1  
subversion-debuginfo-1.8.15-2.23.1  
subversion-tools-1.8.15-2.23.1  
subversion-ruby-1.8.15-2.23.1  
subversion-perl-debuginfo-1.8.15-2.23.1  
subversion-ruby-debuginfo-1.8.15-2.23.1

## 144109 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2369-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7758

### Description

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

openSUSE-SU-2015:2369-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00117.html>

SuSE Linux 13.1  
x86\_64  
gummi-0.6.5-2.4.1  
gummi-debugsource-0.6.5-2.4.1  
gummi-debuginfo-0.6.5-2.4.1

i586  
gummi-0.6.5-2.4.1  
gummi-debugsource-0.6.5-2.4.1  
gummi-debuginfo-0.6.5-2.4.1

SuSE Linux 13.2  
x86\_64  
gummi-0.6.5-5.3.1  
gummi-debuginfo-0.6.5-5.3.1  
gummi-debugsource-0.6.5-5.3.1

i586  
gummi-0.6.5-5.3.1  
gummi-debuginfo-0.6.5-5.3.1  
gummi-debugsource-0.6.5-5.3.1

## 144111 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2356-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-5330, CVE-2015-7540, CVE-2015-8467

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2356-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00107.html>

SuSE Linux 13.1  
i586  
libsamdb-4.1.22-3.46.1  
pytalloc-2.1.5-7.10.1  
libwbclient-4.1.22-3.46.1  
libdcerpc-atsvc-4.1.22-3.46.1  
samba-debugsource-4.1.22-3.46.1  
libsmbclient-raw-4.1.22-3.46.1  
python-tdb-debuginfo-1.3.8-4.7.1  
python-tdb-1.3.8-4.7.1  
samba-4.1.22-3.46.1  
libsamba-policy-devel-4.1.22-3.46.1  
libndr-standard-devel-4.1.22-3.46.1  
libsmbsharemodes-4.1.22-3.46.1  
libsmbclient-4.1.22-3.46.1  
libsamba-credentials-4.1.22-3.46.1  
libndr-standard-4.1.22-3.46.1  
libldb-devel-1.1.24-3.7.1  
libsmbconf-4.1.22-3.46.1  
libdcerpc-4.1.22-3.46.1

libtdb1-1.3.8-4.7.1  
libdcerpc-devel-4.1.22-3.46.1  
libtevent-util0-debuginfo-4.1.22-3.46.1  
samba-pidl-4.1.22-3.46.1  
libtalloc-devel-2.1.5-7.10.1  
libwbclient-devel-4.1.22-3.46.1  
tevent-debugsource-0.9.26-4.7.1  
libsmbclient-raw0-debuginfo-4.1.22-3.46.1  
libsamba-hostconfig-devel-4.1.22-3.46.1  
samba-python-4.1.22-3.46.1  
libndr-krb5pac0-debuginfo-4.1.22-3.46.1  
pyldb-debuginfo-1.1.24-3.7.1  
libregistry0-4.1.22-3.46.1  
python-tevent-0.9.26-4.7.1  
tdb-debugsource-1.3.8-4.7.1  
libdcerpc-binding0-4.1.22-3.46.1  
libregistry-devel-4.1.22-3.46.1  
pyldb-1.1.24-3.7.1  
libndr-standard0-4.1.22-3.46.1  
libtdb-devel-1.3.8-4.7.1  
samba-libs-4.1.22-3.46.1  
libndr-devel-4.1.22-3.46.1  
libtevent-util-devel-4.1.22-3.46.1  
libsamba-util0-debuginfo-4.1.22-3.46.1  
pytalloc-devel-2.1.5-7.10.1  
libnetapi0-4.1.22-3.46.1  
libsmbldap-devel-4.1.22-3.46.1  
libsamba-credentials-devel-4.1.22-3.46.1  
libtevent0-debuginfo-0.9.26-4.7.1  
libnetapi0-debuginfo-4.1.22-3.46.1  
libgensec0-4.1.22-3.46.1  
libndr-nbt0-4.1.22-3.46.1  
samba-debuginfo-4.1.22-3.46.1  
libtalloc2-debuginfo-2.1.5-7.10.1  
libsamba-hostconfig0-debuginfo-4.1.22-3.46.1  
libsmbconf-devel-4.1.22-3.46.1  
samba-winbind-debuginfo-4.1.22-3.46.1  
libsmbconf0-4.1.22-3.46.1  
libdcerpc-samr-devel-4.1.22-3.46.1  
libpdb0-debuginfo-4.1.22-3.46.1  
samba-client-debuginfo-4.1.22-3.46.1  
ldb-debugsource-1.1.24-3.7.1  
libndr-nbt-devel-4.1.22-3.46.1  
libpdb-devel-4.1.22-3.46.1  
libregistry0-debuginfo-4.1.22-3.46.1  
talloc-debugsource-2.1.5-7.10.1  
libtevent-util0-4.1.22-3.46.1  
libsmbclient-devel-4.1.22-3.46.1  
libsamba-hostconfig0-4.1.22-3.46.1  
libsamdb-devel-4.1.22-3.46.1  
libtdb1-debuginfo-1.3.8-4.7.1  
libtevent0-0.9.26-4.7.1  
samba-test-devel-4.1.22-3.46.1  
libsamdb0-debuginfo-4.1.22-3.46.1  
libsamba-policy0-debuginfo-4.1.22-3.46.1  
libwbclient0-4.1.22-3.46.1  
libnetapi-devel-4.1.22-3.46.1  
libtevent-devel-0.9.26-4.7.1  
libsmbclient0-4.1.22-3.46.1  
tdb-tools-1.3.8-4.7.1



libdcerpc0-4.1.22-3.46.1  
libdcerpc-atvc0-4.1.22-3.46.1  
samba-test-4.1.22-3.46.1  
pytalloc-debuginfo-2.1.5-7.10.1  
samba-test-debuginfo-4.1.22-3.46.1  
samba-client-4.1.22-3.46.1  
libsamba-policy0-4.1.22-3.46.1  
libndr0-debuginfo-4.1.22-3.46.1  
libgensec-devel-4.1.22-3.46.1  
libdcerpc-samr0-debuginfo-4.1.22-3.46.1  
libndr-nbt0-debuginfo-4.1.22-3.46.1  
libpdb0-4.1.22-3.46.1  
libndr0-4.1.22-3.46.1  
libndr-krb5pac0-4.1.22-3.46.1  
libgensec0-debuginfo-4.1.22-3.46.1  
libdcerpc-samr0-4.1.22-3.46.1  
ldb-tools-debuginfo-1.1.24-3.7.1  
samba-core-devel-4.1.22-3.46.1  
samba-python-debuginfo-4.1.22-3.46.1  
libndr-krb5pac-devel-4.1.22-3.46.1  
libsamba-util0-4.1.22-3.46.1  
libldb1-1.1.24-3.7.1  
libsmbldap0-4.1.22-3.46.1  
libsamba-credentials0-debuginfo-4.1.22-3.46.1  
libdcerpc-atvc-devel-4.1.22-3.46.1  
ldb-tools-1.1.24-3.7.1  
libsmbldap0-debuginfo-4.1.22-3.46.1  
libsmbsharemodes0-4.1.22-3.46.1  
tdb-tools-debuginfo-1.3.8-4.7.1  
libldb1-debuginfo-1.1.24-3.7.1  
libtalloc2-2.1.5-7.10.1  
samba-winbind-4.1.22-3.46.1  
libsmbclient-raw-devel-4.1.22-3.46.1  
libdcerpc-binding0-debuginfo-4.1.22-3.46.1  
samba-libs-debuginfo-4.1.22-3.46.1  
pyldb-devel-1.1.24-3.7.1  
libsmbsharemodes-devel-4.1.22-3.46.1  
python-tevent-debuginfo-0.9.26-4.7.1  
libsamba-util-devel-4.1.22-3.46.1

noarch  
samba-doc-4.1.22-3.46.1

x86\_64  
libsmbclient-raw0-debuginfo-32bit-4.1.22-3.46.1  
libsmbldap0-debuginfo-4.1.22-3.46.1  
libsamba-util-devel-4.1.22-3.46.1  
pyldb-1.1.24-3.7.1  
samba-winbind-4.1.22-3.46.1  
libndr-nbt0-debuginfo-4.1.22-3.46.1  
libsmbldap0-32bit-4.1.22-3.46.1  
libnetapi0-debuginfo-4.1.22-3.46.1  
libsamba-hostconfig-devel-4.1.22-3.46.1  
libtevent0-32bit-0.9.26-4.7.1  
libsmbclient0-debuginfo-32bit-4.1.22-3.46.1  
libwbclient0-4.1.22-3.46.1  
pytalloc-devel-2.1.5-7.10.1  
libndr0-debuginfo-4.1.22-3.46.1  
libndr0-4.1.22-3.46.1  
libsamba-policy0-debuginfo-4.1.22-3.46.1

libtdb1-1.3.8-4.7.1  
libtalloc2-2.1.5-7.10.1  
python-tevent-0.9.26-4.7.1  
libpdb0-debuginfo-32bit-4.1.22-3.46.1  
libnetapi0-debuginfo-32bit-4.1.22-3.46.1  
libdcerpc-atsvc0-debuginfo-32bit-4.1.22-3.46.1  
libsmbconf0-4.1.22-3.46.1  
libsamba-policy0-debuginfo-32bit-4.1.22-3.46.1  
pytalloc-2.1.5-7.10.1  
libdcerpc-devel-4.1.22-3.46.1  
libwbclient0-debuginfo-32bit-4.1.22-3.46.1  
libsmbconf-devel-4.1.22-3.46.1  
libsmbclient-devel-4.1.22-3.46.1  
tevent-debugsource-0.9.26-4.7.1  
libdcerpc-samr0-32bit-4.1.22-3.46.1  
libdcerpc0-32bit-4.1.22-3.46.1  
libsmbconf0-32bit-4.1.22-3.46.1  
libdcerpc-samr-devel-4.1.22-3.46.1  
libsamba-util0-32bit-4.1.22-3.46.1  
samba-test-debuginfo-4.1.22-3.46.1  
libsamba-credentials0-debuginfo-4.1.22-3.46.1  
libsamba-credentials0-debuginfo-32bit-4.1.22-3.46.1  
libldb-devel-1.1.24-3.7.1  
libldb1-1.1.24-3.7.1  
libtevent-devel-0.9.26-4.7.1  
libsmbsharemodes0-4.1.22-3.46.1  
libgensec0-debuginfo-4.1.22-3.46.1  
libtevent-util-devel-4.1.22-3.46.1  
libtdb-devel-1.3.8-4.7.1  
libsamba-hostconfig0-32bit-4.1.22-3.46.1  
libregistry0-debuginfo-4.1.22-3.46.1  
libndr-nbt0-32bit-4.1.22-3.46.1  
samba-winbind-debuginfo-32bit-4.1.22-3.46.1  
samba-core-devel-4.1.22-3.46.1  
tdb-tools-debuginfo-1.3.8-4.7.1  
libpdb0-4.1.22-3.46.1  
pytalloc-32bit-2.1.5-7.10.1  
pyldb-32bit-1.1.24-3.7.1  
libpdb-devel-4.1.22-3.46.1  
libsmbclient0-4.1.22-3.46.1  
libsmbclient-raw-devel-4.1.22-3.46.1  
libdcerpc0-debuginfo-4.1.22-3.46.1  
libtevent-util0-debuginfo-4.1.22-3.46.1  
libgensec0-4.1.22-3.46.1  
libndr-nbt-devel-4.1.22-3.46.1  
samba-libs-4.1.22-3.46.1  
libwbclient-devel-4.1.22-3.46.1  
libndr-krb5pac0-4.1.22-3.46.1  
python-tdb-debuginfo-1.3.8-4.7.1  
libndr-standard0-32bit-4.1.22-3.46.1  
samba-debuginfo-4.1.22-3.46.1  
samba-client-debuginfo-4.1.22-3.46.1  
libdcerpc-binding0-debuginfo-32bit-4.1.22-3.46.1  
samba-libs-debuginfo-32bit-4.1.22-3.46.1  
libsamba-policy0-4.1.22-3.46.1  
libsamba-credentials0-4.1.22-3.46.1  
libsamba-hostconfig0-debuginfo-32bit-4.1.22-3.46.1  
python-tevent-32bit-0.9.26-4.7.1  
libsmbclient-raw0-debuginfo-4.1.22-3.46.1  
libldb1-debuginfo-32bit-1.1.24-3.7.1

libregistry0-32bit-4.1.22-3.46.1  
python-tdb-1.3.8-4.7.1  
libdcerpc-samr0-debuginfo-32bit-4.1.22-3.46.1  
libdcerpc-binding0-debuginfo-4.1.22-3.46.1  
libtdb1-debuginfo-1.3.8-4.7.1  
libsmbldap0-debuginfo-32bit-4.1.22-3.46.1  
pyldb-debuginfo-1.1.24-3.7.1  
libnetapi0-32bit-4.1.22-3.46.1  
libsmbclient0-32bit-4.1.22-3.46.1  
libtalloc2-debuginfo-32bit-2.1.5-7.10.1  
libndr-standard-devel-4.1.22-3.46.1  
samba-libs-32bit-4.1.22-3.46.1  
pyldb-devel-1.1.24-3.7.1  
libtevent-util0-32bit-4.1.22-3.46.1  
libndr-krb5pac0-debuginfo-4.1.22-3.46.1

SuSE Linux 13.2

i586

libsmbconf-devel-4.1.22-21.1

## 144114 - SuSE Linux 13.2 openSUSE-SU-2015:2367-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8327, CVE-2015-8560

### Description

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

openSUSE-SU-2015:2367-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00115.html>

SuSE Linux 13.2

x86\_64

cups-filters-cups-browsed-1.0.58-2.11.1  
cups-filters-debuginfo-1.0.58-2.11.1  
cups-filters-ghostscript-debuginfo-1.0.58-2.11.1  
cups-filters-ghostscript-1.0.58-2.11.1  
cups-filters-devel-1.0.58-2.11.1  
cups-filters-cups-browsed-debuginfo-1.0.58-2.11.1  
cups-filters-debugsource-1.0.58-2.11.1  
cups-filters-foomatic-rip-1.0.58-2.11.1  
cups-filters-foomatic-rip-debuginfo-1.0.58-2.11.1  
cups-filters-1.0.58-2.11.1

i586

cups-filters-cups-browsed-1.0.58-2.11.1  
cups-filters-debuginfo-1.0.58-2.11.1  
cups-filters-ghostscript-debuginfo-1.0.58-2.11.1  
cups-filters-ghostscript-1.0.58-2.11.1  
cups-filters-devel-1.0.58-2.11.1  
cups-filters-cups-browsed-debuginfo-1.0.58-2.11.1  
cups-filters-debugsource-1.0.58-2.11.1  
cups-filters-foomatic-rip-1.0.58-2.11.1

cups-filters-foomatic-rip-debuginfo-1.0.58-2.11.1  
cups-filters-1.0.58-2.11.1

## 144116 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2372-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-0191, CVE-2014-3660, CVE-2015-1819, CVE-2015-5312, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7941, CVE-2015-7942, CVE-2015-8035, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2372-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00120.html>

### SuSE Linux 13.1

i586  
libxml2-tools-debuginfo-2.9.3-2.19.1  
libxml2-tools-2.9.3-2.19.1  
libxml2-2-debuginfo-2.9.3-2.19.1  
python-libxml2-2.9.3-2.19.1  
libxml2-debugsource-2.9.3-2.19.1  
libxml2-devel-2.9.3-2.19.1  
python-libxml2-debugsource-2.9.3-2.19.1  
python-libxml2-debuginfo-2.9.3-2.19.1  
libxml2-2-2.9.3-2.19.1

### noarch

libxml2-doc-2.9.3-2.19.1

### x86\_64

libxml2-tools-debuginfo-2.9.3-2.19.1  
libxml2-tools-2.9.3-2.19.1  
libxml2-2-debuginfo-2.9.3-2.19.1  
python-libxml2-2.9.3-2.19.1  
libxml2-debugsource-2.9.3-2.19.1  
libxml2-devel-2.9.3-2.19.1  
python-libxml2-debugsource-2.9.3-2.19.1  
python-libxml2-debuginfo-2.9.3-2.19.1  
libxml2-2-32bit-2.9.3-2.19.1  
libxml2-2-2.9.3-2.19.1  
libxml2-2-debuginfo-32bit-2.9.3-2.19.1  
libxml2-devel-32bit-2.9.3-2.19.1

### SuSE Linux 13.2

i586  
libxml2-debugsource-2.9.3-7.4.1  
libxml2-devel-2.9.3-7.4.1  
libxml2-tools-2.9.3-7.4.1  
python-libxml2-2.9.3-7.4.1  
libxml2-tools-debuginfo-2.9.3-7.4.1  
python-libxml2-debugsource-2.9.3-7.4.1  
libxml2-2-debuginfo-2.9.3-7.4.1

libxml2-2-2.9.3-7.4.1  
python-libxml2-debuginfo-2.9.3-7.4.1

noarch  
libxml2-doc-2.9.3-7.4.1

x86\_64  
libxml2-debugsource-2.9.3-7.4.1  
libxml2-devel-2.9.3-7.4.1  
libxml2-tools-2.9.3-7.4.1  
python-libxml2-2.9.3-7.4.1  
libxml2-2-debuginfo-32bit-2.9.3-7.4.1  
libxml2-tools-debuginfo-2.9.3-7.4.1  
python-libxml2-debugsource-2.9.3-7.4.1  
libxml2-2-debuginfo-2.9.3-7.4.1  
libxml2-devel-32bit-2.9.3-7.4.1  
libxml2-2-2.9.3-7.4.1  
libxml2-2-32bit-2.9.3-7.4.1  
python-libxml2-debuginfo-2.9.3-7.4.1

### 181729 - FreeBSD dpkg Stack-based Buffer Overflow (876768aa-ab1e-11e5-8a30-5453ed2e2b49)

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

Risk Level: High

CVE: CVE-2015-0860

#### Description

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

dpkg -- stack-based buffer overflow (876768aa-ab1e-11e5-8a30-5453ed2e2b49)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/876768aa-ab1e-11e5-8a30-5453ed2e2b49.html>

Affected packages:

dpkg < 1.16.17

dpkg < 1.17.26

dpkg < 1.18.4

### 181730 - FreeBSD ffmpeg Multiple Vulnerabilities (4bae544d-06a3-4352-938c-b3bcbca89298)

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

Risk Level: High

CVE: CVE-2015-8662, CVE-2015-8663

#### Description

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

ffmpeg -- multiple vulnerabilities (4bae544d-06a3-4352-938c-b3bcbca89298)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/4bae544d-06a3-4352-938c-b3bcbca89298.html>

Affected packages:

2.8,1 <= ffmpeg < 2.8.4,1

ffmpeg < 2.7.4,1

ffmpeg26 < 2.6.6

ffmpeg25 < 2.5.9

ffmpeg24 < 2.4.12

kodi < 16.0

mplayer < 1.2.r20151219\_1

mencoder < 1.2.r20151219\_1

### 19450 - (SOL17566) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7704

#### Description

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

#### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the NTP client. Successful exploitation could allow an attacker to cause a denial of service condition, disabling synchronization with the NTP server.

### 19466 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.106

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

Risk Level: Medium

CVE: CVE-2015-6792, CVE-2015-8664

#### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

#### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws are due to an incorrect malformed web content processing. Successful exploitation could allow an attacker to remotely execute arbitrary code, to cause a denial of service condition or to retrieve sensitive data.

### 19467 - Google Chrome Multiple Vulnerabilities Prior To 47.0.2526.106

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-6792, CVE-2015-8664

#### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

#### Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws are due to an incorrect malformed web content processing. Successful exploitation could allow an attacker to remotely execute arbitrary code, to cause a denial of service condition or to retrieve sensitive data.

## 144106 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2375-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2375-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00123.html>

#### SuSE Linux 13.1

##### x86\_64

grub2-debuginfo-2.00-39.11.1  
grub2-2.00-39.11.1  
grub2-x86\_64-efi-debuginfo-2.00-39.11.1  
grub2-x86\_64-efi-2.00-39.11.1  
grub2-i386-pc-2.00-39.11.1  
grub2-i386-pc-debuginfo-2.00-39.11.1  
grub2-debugsource-2.00-39.11.1

##### i586

grub2-debuginfo-2.00-39.11.1  
grub2-i386-efi-debuginfo-2.00-39.11.1  
grub2-2.00-39.11.1  
grub2-i386-pc-2.00-39.11.1  
grub2-i386-pc-debuginfo-2.00-39.11.1  
grub2-i386-efi-2.00-39.11.1  
grub2-debugsource-2.00-39.11.1

#### SuSE Linux 13.2

##### i586

grub2-branding-upstream-2.02~beta2-20.13.1  
grub2-2.02~beta2-20.13.1  
grub2-debugsource-2.02~beta2-20.13.1  
grub2-i386-pc-2.02~beta2-20.13.1  
grub2-i386-efi-2.02~beta2-20.13.1  
grub2-debuginfo-2.02~beta2-20.13.1

##### noarch

grub2-snapper-plugin-2.02~beta2-20.13.1

##### x86\_64

grub2-branding-upstream-2.02~beta2-20.13.1  
grub2-2.02~beta2-20.13.1  
grub2-x86\_64-xen-2.02~beta2-20.13.1  
grub2-x86\_64-efi-2.02~beta2-20.13.1  
grub2-debugsource-2.02~beta2-20.13.1

grub2-i386-pc-2.02~beta2-20.13.1  
grub2-debuginfo-2.02~beta2-20.13.1

### 144117 - SuSE Linux 13.2 openSUSE-SU-2015:2371-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5291

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2371-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00119.html>

SuSE Linux 13.2

x86\_64

libpolarssl7-debuginfo-1.3.9-11.1

polarssl-devel-1.3.9-11.1

libpolarssl7-1.3.9-11.1

i586

libpolarssl7-debuginfo-1.3.9-11.1

polarssl-devel-1.3.9-11.1

libpolarssl7-1.3.9-11.1

### 144118 - SuSE Linux 11.4 openSUSE-SU-2015:2392-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2392-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00132.html>

SuSE Linux 11.4

x86\_64

grub2-1.98-14.1

grub2-debugsource-1.98-14.1

grub2-debuginfo-1.98-14.1

i586

grub2-1.98-14.1

grub2-debugsource-1.98-14.1

grub2-debuginfo-1.98-14.1



## 190130 - Fedora Linux 23 FEDORA-2015-6dec4e6d5f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2009-0689

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-6dec4e6d5f

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174612.html>

Fedora Core 23

mono-4.0.5-2.fc23

## 19040 - (SOL17155) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-4638

### Description

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

### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Traffic Management Microkernel. Successful exploitation could allow an attacker to cause a denial of service condition.

## 19445 - (SOL17515) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7855

### Description

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

### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ntpd process. Successful exploitation could allow an attacker to cause a denial of service condition.

## 19446 - (SOL17517) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7701

#### Description

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

#### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ntpd process. Successful exploitation could allow an attacker to cause a denial of service condition.

### **19448 - (SOL17526) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7848

#### Description

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

#### Observation

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

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

### **19449 - (SOL17527) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7705

#### Description

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

#### Observation

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

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

### **144108 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2364-1 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-8000

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2364-1

## Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00112.html>

### SuSE Linux 13.1

i586

bind-chrootenv-9.9.4P2-2.20.1

bind-lwresd-9.9.4P2-2.20.1

bind-libs-9.9.4P2-2.20.1

bind-utils-debuginfo-9.9.4P2-2.20.1

bind-debuginfo-9.9.4P2-2.20.1

bind-lwresd-debuginfo-9.9.4P2-2.20.1

bind-9.9.4P2-2.20.1

bind-libs-debuginfo-9.9.4P2-2.20.1

bind-utils-9.9.4P2-2.20.1

bind-devel-9.9.4P2-2.20.1

bind-debugsource-9.9.4P2-2.20.1

noarch

bind-doc-9.9.4P2-2.20.1

x86\_64

bind-libs-debuginfo-9.9.4P2-2.20.1

bind-libs-debuginfo-32bit-9.9.4P2-2.20.1

bind-libs-32bit-9.9.4P2-2.20.1

bind-lwresd-debuginfo-9.9.4P2-2.20.1

bind-debugsource-9.9.4P2-2.20.1

bind-utils-9.9.4P2-2.20.1

bind-chrootenv-9.9.4P2-2.20.1

bind-libs-9.9.4P2-2.20.1

bind-debuginfo-9.9.4P2-2.20.1

bind-9.9.4P2-2.20.1

bind-devel-9.9.4P2-2.20.1

bind-utils-debuginfo-9.9.4P2-2.20.1

bind-lwresd-9.9.4P2-2.20.1

### SuSE Linux 13.2

i586

bind-libs-debuginfo-9.9.6P1-2.13.1

bind-utils-debuginfo-9.9.6P1-2.13.1

bind-libs-9.9.6P1-2.13.1

bind-utils-9.9.6P1-2.13.1

bind-lwresd-9.9.6P1-2.13.1

bind-9.9.6P1-2.13.1

bind-chrootenv-9.9.6P1-2.13.1

bind-debugsource-9.9.6P1-2.13.1

bind-devel-9.9.6P1-2.13.1

bind-lwresd-debuginfo-9.9.6P1-2.13.1

bind-debuginfo-9.9.6P1-2.13.1

noarch

bind-doc-9.9.6P1-2.13.1

x86\_64

bind-debuginfo-9.9.6P1-2.13.1

bind-libs-9.9.6P1-2.13.1

bind-lwresd-9.9.6P1-2.13.1

bind-utils-debuginfo-9.9.6P1-2.13.1  
bind-debugsource-9.9.6P1-2.13.1  
bind-9.9.6P1-2.13.1  
bind-chrootenv-9.9.6P1-2.13.1  
bind-libs-32bit-9.9.6P1-2.13.1  
bind-devel-9.9.6P1-2.13.1  
bind-utils-9.9.6P1-2.13.1  
bind-libs-debuginfo-32bit-9.9.6P1-2.13.1  
bind-lwresd-debuginfo-9.9.6P1-2.13.1  
bind-libs-debuginfo-9.9.6P1-2.13.1

## 144110 - SuSE Linux 11.4 openSUSE-SU-2015:2391-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2015:2391-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00131.html>

SuSE Linux 11.4

i586

bind-chrootenv-9.9.4P2-72.1  
bind-utils-9.9.4P2-72.1  
bind-9.9.4P2-72.1  
bind-libs-9.9.4P2-72.1  
bind-devel-9.9.4P2-72.1  
bind-libs-debuginfo-9.9.4P2-72.1  
bind-lwresd-debuginfo-9.9.4P2-72.1  
bind-debugsource-9.9.4P2-72.1  
bind-utils-debuginfo-9.9.4P2-72.1  
bind-lwresd-9.9.4P2-72.1  
bind-debuginfo-9.9.4P2-72.1

noarch

bind-doc-9.9.4P2-72.1

x86\_64

bind-utils-9.9.4P2-72.1  
bind-debuginfo-9.9.4P2-72.1  
bind-lwresd-debuginfo-9.9.4P2-72.1  
bind-chrootenv-9.9.4P2-72.1  
bind-debugsource-9.9.4P2-72.1  
bind-libs-debuginfo-9.9.4P2-72.1  
bind-libs-debuginfo-32bit-9.9.4P2-72.1  
bind-libs-32bit-9.9.4P2-72.1  
bind-lwresd-9.9.4P2-72.1  
bind-9.9.4P2-72.1  
bind-devel-9.9.4P2-72.1  
bind-utils-debuginfo-9.9.4P2-72.1  
bind-libs-9.9.4P2-72.1

## 144115 - SuSE SLES 12, SLED 12 SUSE-SU-2015:2384-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2012-2150

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2015:2384-1

### Observation

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

<http://lists.suse.com/pipermail/sle-security-updates/2015-December/001765.html>

SuSE SLED 12

x86\_64

xfspgcs-debuginfo-3.2.1-3.5

xfspgcs-3.2.1-3.5

xfspgcs-debugsource-3.2.1-3.5

SuSE SLES 12

x86\_64

xfspgcs-debuginfo-3.2.1-3.5

xfspgcs-3.2.1-3.5

xfspgcs-debugsource-3.2.1-3.5

## 181732 - FreeBSD phpMyAdmin Path Disclosure Vulnerability (88f75070-abcf-11e5-83d3-6805ca0b3d42)

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

Risk Level: Medium

CVE: CVE-2015-8669

### Description

The scan detected that the host is missing the following update:  
phpMyAdmin -- path disclosure vulnerability (88f75070-abcf-11e5-83d3-6805ca0b3d42)

### Observation

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

<http://www.vuxml.org/freebsd/88f75070-abcf-11e5-83d3-6805ca0b3d42.html>

Affected packages:

4.5.0 <= phpMyAdmin < 4.5.3.1

## 190136 - Fedora Linux 22 FEDORA-2015-e278e12ebc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-e278e12ebc

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174520.html>  
<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174519.html>

Fedora Core 22

bind99-9.9.8-1.P2.fc22  
dhcp-4.3.2-6.fc22

### **19447 - (SOL17529) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5  
Risk Level: Medium  
CVE: CVE-2015-7703

#### Description

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

#### Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ntpq component. Successful exploitation could allow an attacker to modify configuration directives for the driftfile and pid files.

### **19451 - (SOL17528) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5  
Risk Level: Medium  
CVE: CVE-2015-7850

#### Description

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

#### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ntpd process. Successful exploitation could allow an attacker to cause a denial of service condition.

### **19452 - (SOL17530) F5 BIG-IP NTP Vulnerabilities**

Category: SSH Module -> NonIntrusive -> F5  
Risk Level: Medium  
CVE: CVE-2015-7691, CVE-2015-7692, CVE-2015-7702

#### Description

Multiple denial of service vulnerabilities are present in some versions of F5 BIG-IP systems

### Observation

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

Multiple denial of service vulnerabilities are present in some versions of F5 BIG-IP systems. The flaws lie in the ntpd process. Successful exploitation could allow an attacker to cause a denial of service condition.

### **19453 - (SOL17516) F5 BIG-IP NTP Vulnerability**

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7852

### Description

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

### Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the ntpq process. Successful exploitation could allow an attacker to cause a denial of service condition.

### **88731 - Slackware Linux 14.1 SSA:2015-357-01 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:2015-357-01

### Observation

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

For more information see:

<http://www.slackware.com/security/viewer.php?l=slackware-security&y=2015&m=slackware-security.359890>

Slackware 14.1

x86\_64

mozilla-thunderbird-38.5.0-x86\_64-1

### **144113 - SuSE Linux 13.2 openSUSE-SU-2015:2355-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

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

openSUSE-SU-2015:2355-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2015-12/msg00106.html>

SuSE Linux 13.2

i586

glibc-obsolete-2.19-16.18.1  
glibc-extra-2.19-16.18.1  
glibc-utils-debuginfo-2.19-16.18.1  
glibc-2.19-16.18.1  
glibc-extra-debuginfo-2.19-16.18.1  
glibc-utils-2.19-16.18.1  
nscd-2.19-16.18.1  
glibc-locale-2.19-16.18.1  
nscd-debuginfo-2.19-16.18.1  
glibc-devel-2.19-16.18.1  
glibc-devel-static-2.19-16.18.1  
glibc-profile-2.19-16.18.1  
glibc-obsolete-debuginfo-2.19-16.18.1  
glibc-debuginfo-2.19-16.18.1  
glibc-debugsource-2.19-16.18.1  
glibc-locale-debuginfo-2.19-16.18.1  
glibc-devel-debuginfo-2.19-16.18.1  
glibc-utils-debugsource-2.19-16.18.1

noarch

glibc-info-2.19-16.18.1  
glibc-html-2.19-16.18.1  
glibc-i18ndata-2.19-16.18.1

x86\_64

glibc-utils-debuginfo-32bit-2.19-16.18.1  
glibc-extra-2.19-16.18.1  
glibc-utils-debuginfo-2.19-16.18.1  
glibc-2.19-16.18.1  
glibc-extra-debuginfo-2.19-16.18.1  
glibc-utils-2.19-16.18.1  
nscd-2.19-16.18.1  
glibc-locale-2.19-16.18.1  
nscd-debuginfo-2.19-16.18.1  
glibc-devel-2.19-16.18.1  
glibc-utils-32bit-2.19-16.18.1  
glibc-devel-static-2.19-16.18.1  
glibc-profile-2.19-16.18.1  
glibc-debuginfo-2.19-16.18.1  
glibc-debugsource-2.19-16.18.1  
glibc-locale-debuginfo-2.19-16.18.1  
glibc-devel-debuginfo-2.19-16.18.1  
glibc-utils-debugsource-2.19-16.18.1

### 181731 - FreeBSD inspircd DoS (b808c3a8-ae30-11e5-b864-14dae9d210b8)

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

Risk Level: Low

CVE: CVE-2015-8702

#### Description

The scan detected that the host is missing the following update:  
inspircd -- DoS (b808c3a8-ae30-11e5-b864-14dae9d210b8)



### Observation

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

<http://www.vuxml.org/freebsd/b808c3a8-ae30-11e5-b864-14dae9d210b8.html>

Affected packages:  
inspircd < 2.0.19

### **181733 - FreeBSD Ruby Unsafe Tainted String Vulnerability (3b50881d-1860-4721-aab1-503290e23f6c)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-2015-7551

### Description

The scan detected that the host is missing the following update:  
Ruby -- unsafe tainted string vulnerability (3b50881d-1860-4721-aab1-503290e23f6c)

### Observation

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

<http://www.vuxml.org/freebsd/3b50881d-1860-4721-aab1-503290e23f6c.html>

Affected packages:  
2.0.0,1 <= ruby < 2.0.0.648,1  
2.1.0,1 <= ruby < 2.1.8,1  
2.2.0,1 <= ruby < 2.2.4,1

### **181734 - FreeBSD mediawiki Multiple Vulnerabilities (f36bbd66-aa44-11e5-8f5c-002590263bf5)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes  
Risk Level: Low  
CVE: CVE-2015-8622, CVE-2015-8623, CVE-2015-8624, CVE-2015-8625, CVE-2015-8626, CVE-2015-8627, CVE-2015-8628

### Description

The scan detected that the host is missing the following update:  
mediawiki -- multiple vulnerabilities (f36bbd66-aa44-11e5-8f5c-002590263bf5)

### Observation

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

<http://www.vuxml.org/freebsd/f36bbd66-aa44-11e5-8f5c-002590263bf5.html>

Affected packages:  
mediawiki123 < 1.23.12  
mediawiki124 < 1.24.5  
mediawiki125 < 1.25.4  
mediawiki126 < 1.26.1

### **181735 - FreeBSD mantis Information Disclosure Vulnerability (e1b5318c-aa4d-11e5-8f5c-002590263bf5)**

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

Risk Level: Low

CVE: CVE-2015-5059

#### Description

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

mantis -- information disclosure vulnerability (e1b5318c-aa4d-11e5-8f5c-002590263bf5)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/e1b5318c-aa4d-11e5-8f5c-002590263bf5.html>

Affected packages:

mantis < 1.2.19\_1

### **181736 - FreeBSD NSS MD5 Downgrade In TLS 1.2 Signatures (10f7bc76-0335-4a88-b391-0b05b3a8ce1c)**

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

Risk Level: Low

CVE: CVE-2015-7575

#### Description

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

NSS -- MD5 downgrade in TLS 1.2 signatures (10f7bc76-0335-4a88-b391-0b05b3a8ce1c)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/10f7bc76-0335-4a88-b391-0b05b3a8ce1c.html>

Affected packages:

3.20 <= nss < 3.20.2

3.20 <= linux-c6-nss < 3.20.2

nss < 3.19.2.2

linux-c6-nss < 3.19.2.2

linux-firefox < 43.0.2,1

linux-thunderbird < 38.5.1

linux-seamonkey < 2.40

### **190126 - Fedora Linux 23 FEDORA-2015-1ca595f821 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-8466

#### Description

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

FEDORA-2015-1ca595f821

#### Observation

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

For more information see:

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174374.html>

Fedora Core 23

openstack-swift-plugin-swift3-1.9-1.fc23

#### **190127 - Fedora Linux 23 FEDORA-2015-3868cfa17b Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-8540

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-3868cfa17b

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174435.html>

Fedora Core 23

libpng10-1.0.66-1.fc23

#### **190128 - Fedora Linux 23 FEDORA-2015-277cc63d9f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-7542

##### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-277cc63d9f

##### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174484.html>

Fedora Core 23

gwenhywfar-4.13.1-5.fc23

#### **190129 - Fedora Linux 23 FEDORA-2015-eefc5a6762 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5254

## Description

The scan detected that the host is missing the following update:  
FEDORA-2015-eefc5a6762

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174371.html>

Fedora Core 23

activemq-5.6.0-14.fc23

## 190131 - Fedora Linux 23 FEDORA-2015-a3c9048cdd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

## Description

The scan detected that the host is missing the following update:  
FEDORA-2015-a3c9048cdd

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174495.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174493.html>

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174494.html>

Fedora Core 23

php-horde-Horde-Perms-2.1.6-1.fc23

php-horde-Horde-Core-2.22.4-1.fc23

php-horde-Horde-Service-Weather-2.3.1-1.fc23

## 190132 - Fedora Linux 23 FEDORA-2015-6e50918d8e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7543

## Description

The scan detected that the host is missing the following update:  
FEDORA-2015-6e50918d8e

## Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174624.html>

Fedora Core 23

### 190133 - Fedora Linux 23 FEDORA-2015-a7cbc13699 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-a7cbc13699

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174460.html>

Fedora Core 23

nodejs-handlebars-4.0.5-1.fc23

### 190134 - Fedora Linux 23 FEDORA-2015-eef21b972e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2009-5147, CVE-2015-7551

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-eef21b972e

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174610.html>

Fedora Core 23

ruby-2.2.4-47.fc23

### 190135 - Fedora Linux 23 FEDORA-2015-84b1635e90 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7529

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-84b1635e90

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174434.html>

Fedora Core 23

sos-3.2-2.fc23

#### **190137 - Fedora Linux 22 FEDORA-2015-7ca4368b0c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-5254

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-7ca4368b0c

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174537.html>

Fedora Core 22

activemq-5.6.0-14.fc22

#### **190138 - Fedora Linux 23 FEDORA-2015-6d473c95ee Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-7543

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-6d473c95ee

#### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174626.html>

Fedora Core 23

arts-1.5.10-30.fc23

#### **190139 - Fedora Linux 22 FEDORA-2015-8b6882339c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-8b6882339c

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174527.html>

Fedora Core 22

nodejs-handlebars-4.0.5-1.fc22

## **190140 - Fedora Linux 22 FEDORA-2015-0e0879cc8a Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-3223, CVE-2015-5252, CVE-2015-5296, CVE-2015-5299, CVE-2015-7540

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-0e0879cc8a

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174391.html>

Fedora Core 22

samba-4.2.7-0.fc22

## **190141 - Fedora Linux 22 FEDORA-2015-20df66892b Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-7542

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-20df66892b

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174540.html>

Fedora Core 22

gwenhywfar-4.13.1-5.fc22

## 190142 - Fedora Linux 23 FEDORA-2015-30b347dff1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-5313

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-30b347dff1

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174404.html>

Fedora Core 23

libvirt-1.2.18.2-1.fc23

## 190143 - Fedora Linux 22 FEDORA-2015-b406a8e4f2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8504

### Description

The scan detected that the host is missing the following update:  
FEDORA-2015-b406a8e4f2

### Observation

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

<http://lists.fedoraproject.org/pipermail/package-announce/2015-December/174551.html>

Fedora Core 22

qemu-2.3.1-9.fc22

## 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.

## 19479 - (APSB16-01) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

### Update Details



Risk is updated

### 19480 - (APSB16-01) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

#### Update Details

Risk is updated

### 32097 - Oracle Solaris 125358-21 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

#### Update Details

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

### 32098 - Oracle Solaris 125359-21 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

#### Update Details

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

### 33207 - Oracle Solaris 119213-32 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

#### Update Details

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

### 33218 - Oracle Solaris 119214-32 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2009-0689, CVE-2009-2404, CVE-2009-3555, CVE-2010-3170, CVE-2011-3389, CVE-2013-1620, CVE-2013-1739, CVE-2013-1740, CVE-2013-1741, CVE-2013-5605, CVE-2013-5606, CVE-2014-1490, CVE-2014-1491, CVE-2014-1492

#### Update Details

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

### 33093 - Oracle Solaris 148071-19 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3508, CVE-2014-3511, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

#### Update Details

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

### 181567 - FreeBSD mediawiki Multiple Vulnerabilities (6241b5df-42a1-11e5-93ad-002590263bf5)

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

Risk Level: High

CVE: CVE-2013-7444, CVE-2015-6727, CVE-2015-6728, CVE-2015-6729, CVE-2015-6730, CVE-2015-6731, CVE-2015-6733, CVE-2015-6734, CVE-2015-6735, CVE-2015-6736, CVE-2015-6737

#### Update Details

Risk is updated CVE is updated

### 181698 - FreeBSD ffmpeg Multiple Vulnerabilities (b0da85af-21a3-4c15-a137-fe9e4bc86002)

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

Risk Level: High

CVE: CVE-2015-6761, CVE-2015-8216, CVE-2015-8217, CVE-2015-8218, CVE-2015-8219, CVE-2015-8363, CVE-2015-8364, CVE-2015-8365

#### Update Details

FASLScript is updated

### 31558 - Oracle Solaris 119783-33 Update Is Not Installed

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

Risk Level: Medium

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

#### Update Details

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

### 31564 - Oracle Solaris 119784-33 Update Is Not Installed

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

Risk Level: Medium

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

#### Update Details

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

### 181657 - FreeBSD mediawiki Multiple Vulnerabilities (b973a763-7936-11e5-a2a1-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-8001, CVE-2015-8002, CVE-2015-8003, CVE-2015-8004, CVE-2015-8005, CVE-2015-8006, CVE-2015-8007, CVE-2015-8008, CVE-2015-8009

Update Details

Risk is updated CVE is updated

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

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

Risk Level: Medium

CVE: CVE-2015-8213

Update Details

FASLScript is updated

**33091 - Oracle Solaris 148072-19 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2010-4180, CVE-2013-0166, CVE-2013-0169, CVE-2014-0224, CVE-2014-3508, CVE-2014-3511, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated 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 2015 McAfee, Inc.  
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates