

## 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

#### 141361 - Red Hat Enterprise Linux RHSA-2016-2750 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7456, CVE-2014-9767, CVE-2015-2325, CVE-2015-2326, CVE-2015-2327, CVE-2015-2328, CVE-2015-3210, CVE-2015-3217, CVE-2015-5073, CVE-2015-8381, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8388, CVE-2015-8391, CVE-2015-8392, CVE-2015-8395, CVE-2015-8835, CVE-2015-8865, CVE-2015-8866, CVE-2015-8867, CVE-2015-8873, CVE-2015-8874, CVE-2015-8876, CVE-2015-8877, CVE-2015-8879, CVE-2016-1903, CVE-2016-2554, CVE-2016-3074, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4342, CVE-2016-4343, CVE-2016-4473, CVE-2016-4537, CVE-2016-4538, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544, CVE-2016-5093, CVE-2016-5094, CVE-2016-5096, CVE-2016-5114, CVE-2016-5399, CVE-2016-5766, CVE-2016-5767, CVE-2016-5768, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6128, CVE-2016-6207, 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, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2750

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2750.html>

RHEL6S

x86\_64

rh-php56-php-enchant-5.6.25-1.el6

rh-php56-php-common-5.6.25-1.el6

rh-php56-php-recode-5.6.25-1.el6

rh-php56-php-snmp-5.6.25-1.el6

rh-php56-2.3-1.el6

rh-php56-scldevel-2.3-1.el6

rh-php56-php-5.6.25-1.el6

rh-php56-php-ldap-5.6.25-1.el6

rh-php56-php-devel-5.6.25-1.el6

rh-php56-php-dbg-5.6.25-1.el6

rh-php56-php-pdo-5.6.25-1.el6

rh-php56-php-mysqldb-5.6.25-1.el6

rh-php56-php-pspell-5.6.25-1.el6

rh-php56-php-process-5.6.25-1.el6

rh-php56-php-cli-5.6.25-1.el6

rh-php56-runtime-2.3-1.el6

rh-php56-php-odbc-5.6.25-1.el6

rh-php56-php-fpm-5.6.25-1.el6

rh-php56-php-debuginfo-5.6.25-1.el6  
rh-php56-php-tidy-5.6.25-1.el6  
rh-php56-php-gmp-5.6.25-1.el6  
rh-php56-php-xml-5.6.25-1.el6  
rh-php56-php-dba-5.6.25-1.el6  
rh-php56-php-mbstring-5.6.25-1.el6  
rh-php56-php-bcmath-5.6.25-1.el6  
rh-php56-php-xmlrpc-5.6.25-1.el6  
rh-php56-php-embedded-5.6.25-1.el6  
rh-php56-php-opcache-5.6.25-1.el6  
rh-php56-php-soap-5.6.25-1.el6  
rh-php56-php-gd-5.6.25-1.el6  
rh-php56-php-imap-5.6.25-1.el6  
rh-php56-php-pgsql-5.6.25-1.el6  
rh-php56-php-intl-5.6.25-1.el6

noarch

rh-php56-php-pear-1.9.5-4.el6

RHEL6WS

x86\_64

rh-php56-php-enchant-5.6.25-1.el6  
rh-php56-php-common-5.6.25-1.el6  
rh-php56-php-recode-5.6.25-1.el6  
rh-php56-php-snmp-5.6.25-1.el6  
rh-php56-2.3-1.el6  
rh-php56-scldevel-2.3-1.el6  
rh-php56-php-5.6.25-1.el6  
rh-php56-php-ldap-5.6.25-1.el6  
rh-php56-php-devel-5.6.25-1.el6  
rh-php56-php-dbg-5.6.25-1.el6  
rh-php56-php-pdo-5.6.25-1.el6  
rh-php56-php-mysqlnd-5.6.25-1.el6  
rh-php56-php-pspell-5.6.25-1.el6  
rh-php56-php-process-5.6.25-1.el6  
rh-php56-php-cli-5.6.25-1.el6  
rh-php56-runtime-2.3-1.el6  
rh-php56-php-odbc-5.6.25-1.el6  
rh-php56-php-fpm-5.6.25-1.el6  
rh-php56-php-debuginfo-5.6.25-1.el6  
rh-php56-php-tidy-5.6.25-1.el6  
rh-php56-php-gmp-5.6.25-1.el6  
rh-php56-php-xml-5.6.25-1.el6  
rh-php56-php-dba-5.6.25-1.el6  
rh-php56-php-mbstring-5.6.25-1.el6  
rh-php56-php-bcmath-5.6.25-1.el6  
rh-php56-php-xmlrpc-5.6.25-1.el6  
rh-php56-php-embedded-5.6.25-1.el6  
rh-php56-php-opcache-5.6.25-1.el6  
rh-php56-php-soap-5.6.25-1.el6  
rh-php56-php-gd-5.6.25-1.el6  
rh-php56-php-imap-5.6.25-1.el6  
rh-php56-php-pgsql-5.6.25-1.el6  
rh-php56-php-intl-5.6.25-1.el6

noarch

rh-php56-php-pear-1.9.5-4.el6

RHEL7S

x86\_64

rh-php56-php-debuginfo-5.6.25-1.el7  
rh-php56-php-enchant-5.6.25-1.el7  
rh-php56-php-recode-5.6.25-1.el7  
rh-php56-runtime-2.3-1.el7  
rh-php56-2.3-1.el7  
rh-php56-scldevel-2.3-1.el7  
rh-php56-php-5.6.25-1.el7  
rh-php56-php-ldap-5.6.25-1.el7  
rh-php56-php-common-5.6.25-1.el7  
rh-php56-php-devel-5.6.25-1.el7  
rh-php56-php-intl-5.6.25-1.el7  
rh-php56-php-pdo-5.6.25-1.el7  
rh-php56-php-mysqlnd-5.6.25-1.el7  
rh-php56-php-pspell-5.6.25-1.el7  
rh-php56-php-process-5.6.25-1.el7  
rh-php56-php-odbc-5.6.25-1.el7  
rh-php56-php-bcmath-5.6.25-1.el7  
rh-php56-php-fpm-5.6.25-1.el7  
rh-php56-php-embedded-5.6.25-1.el7  
rh-php56-php-gmp-5.6.25-1.el7  
rh-php56-php-soap-5.6.25-1.el7  
rh-php56-php-xml-5.6.25-1.el7  
rh-php56-php-dba-5.6.25-1.el7  
rh-php56-php-cli-5.6.25-1.el7  
rh-php56-php-mbstring-5.6.25-1.el7  
rh-php56-php-opcache-5.6.25-1.el7  
rh-php56-php-xmlrpc-5.6.25-1.el7  
rh-php56-php-gd-5.6.25-1.el7  
rh-php56-php-dbg-5.6.25-1.el7  
rh-php56-php-snmp-5.6.25-1.el7  
rh-php56-php-pgsql-5.6.25-1.el7

noarch

rh-php56-php-pear-1.9.5-4.el7

RHEL7WS

x86\_64

rh-php56-php-debuginfo-5.6.25-1.el7  
rh-php56-php-enchant-5.6.25-1.el7  
rh-php56-php-recode-5.6.25-1.el7  
rh-php56-runtime-2.3-1.el7  
rh-php56-2.3-1.el7  
rh-php56-scldevel-2.3-1.el7  
rh-php56-php-5.6.25-1.el7  
rh-php56-php-ldap-5.6.25-1.el7  
rh-php56-php-common-5.6.25-1.el7  
rh-php56-php-devel-5.6.25-1.el7  
rh-php56-php-intl-5.6.25-1.el7  
rh-php56-php-pdo-5.6.25-1.el7  
rh-php56-php-mysqlnd-5.6.25-1.el7  
rh-php56-php-pspell-5.6.25-1.el7  
rh-php56-php-process-5.6.25-1.el7  
rh-php56-php-odbc-5.6.25-1.el7  
rh-php56-php-bcmath-5.6.25-1.el7  
rh-php56-php-fpm-5.6.25-1.el7  
rh-php56-php-embedded-5.6.25-1.el7  
rh-php56-php-gmp-5.6.25-1.el7  
rh-php56-php-soap-5.6.25-1.el7  
rh-php56-php-xml-5.6.25-1.el7  
rh-php56-php-dba-5.6.25-1.el7

rh-php56-php-cli-5.6.25-1.el7  
rh-php56-php-mbstring-5.6.25-1.el7  
rh-php56-php-opcache-5.6.25-1.el7  
rh-php56-php-xmlrpc-5.6.25-1.el7  
rh-php56-php-gd-5.6.25-1.el7  
rh-php56-php-dbg-5.6.25-1.el7  
rh-php56-php-snmp-5.6.25-1.el7  
rh-php56-php-pgsql-5.6.25-1.el7

noarch  
rh-php56-php-pear-1.9.5-4.el7

## 141362 - Red Hat Enterprise Linux RHSA-2016-2676 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7857, CVE-2016-7858, CVE-2016-7859, CVE-2016-7860, CVE-2016-7861, CVE-2016-7862, CVE-2016-7863, CVE-2016-7864, CVE-2016-7865

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2676

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2676.html>

RHEL5S  
x86\_64  
flash-plugin-11.2.202.644-1.el5\_11

i386  
flash-plugin-11.2.202.644-1.el5\_11

RHEL6D  
x86\_64  
flash-plugin-11.2.202.644-1.el6\_8

i386  
flash-plugin-11.2.202.644-1.el6\_8

RHEL6S  
x86\_64  
flash-plugin-11.2.202.644-1.el6\_8

i386  
flash-plugin-11.2.202.644-1.el6\_8

RHEL6WS  
x86\_64  
flash-plugin-11.2.202.644-1.el6\_8

i386  
flash-plugin-11.2.202.644-1.el6\_8

RHEL5D

x86\_64  
flash-plugin-11.2.202.644-1.el5\_11

i386  
flash-plugin-11.2.202.644-1.el5\_11

## 141364 - Red Hat Enterprise Linux RHSA-2016-2749 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5507, CVE-2016-5616, CVE-2016-5617, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-6664, CVE-2016-8283

### Description

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

RHSA-2016-2749

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2749.html>

### RHEL6S

x86\_64  
rh-mysql56-mysql-devel-5.6.34-2.el6  
rh-mysql56-mysql-5.6.34-2.el6  
rh-mysql56-mysql-server-5.6.34-2.el6  
rh-mysql56-mysql-common-5.6.34-2.el6  
rh-mysql56-mysql-errmsg-5.6.34-2.el6  
rh-mysql56-mysql-bench-5.6.34-2.el6  
rh-mysql56-mysql-test-5.6.34-2.el6  
rh-mysql56-mysql-debuginfo-5.6.34-2.el6  
rh-mysql56-mysql-config-5.6.34-2.el6

### RHEL6WS

x86\_64  
rh-mysql56-mysql-devel-5.6.34-2.el6  
rh-mysql56-mysql-5.6.34-2.el6  
rh-mysql56-mysql-server-5.6.34-2.el6  
rh-mysql56-mysql-common-5.6.34-2.el6  
rh-mysql56-mysql-errmsg-5.6.34-2.el6  
rh-mysql56-mysql-bench-5.6.34-2.el6  
rh-mysql56-mysql-test-5.6.34-2.el6  
rh-mysql56-mysql-debuginfo-5.6.34-2.el6  
rh-mysql56-mysql-config-5.6.34-2.el6

### RHEL7S

x86\_64  
rh-mysql56-mysql-devel-5.6.34-2.el7  
rh-mysql56-mysql-config-5.6.34-2.el7  
rh-mysql56-mysql-5.6.34-2.el7  
rh-mysql56-mysql-server-5.6.34-2.el7  
rh-mysql56-mysql-bench-5.6.34-2.el7  
rh-mysql56-mysql-common-5.6.34-2.el7  
rh-mysql56-mysql-debuginfo-5.6.34-2.el7  
rh-mysql56-mysql-errmsg-5.6.34-2.el7  
rh-mysql56-mysql-test-5.6.34-2.el7

RHEL7WS

x86\_64

rh-mysql56-mysql-devel-5.6.34-2.el7

rh-mysql56-mysql-config-5.6.34-2.el7

rh-mysql56-mysql-5.6.34-2.el7

rh-mysql56-mysql-server-5.6.34-2.el7

rh-mysql56-mysql-bench-5.6.34-2.el7

rh-mysql56-mysql-common-5.6.34-2.el7

rh-mysql56-mysql-debuginfo-5.6.34-2.el7

rh-mysql56-mysql-errmsg-5.6.34-2.el7

rh-mysql56-mysql-test-5.6.34-2.el7

## 144989 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2775-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2014-8158, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8880, CVE-2016-8881, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

### Description

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

SUSE-SU-2016:2775-1

### 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-November/002398.html>

SuSE SLED 12 SP1

x86\_64

libjasper1-32bit-1.900.14-181.1

libjasper1-1.900.14-181.1

libjasper1-debuginfo-32bit-1.900.14-181.1

jasper-debuginfo-1.900.14-181.1

jasper-debugsource-1.900.14-181.1

libjasper1-debuginfo-1.900.14-181.1

SuSE SLES 12 SP2

x86\_64

libjasper1-32bit-1.900.14-181.1

libjasper1-1.900.14-181.1

libjasper1-debuginfo-32bit-1.900.14-181.1

jasper-debuginfo-1.900.14-181.1

jasper-debugsource-1.900.14-181.1

libjasper1-debuginfo-1.900.14-181.1

SuSE SLED 12 SP2

x86\_64

libjasper1-32bit-1.900.14-181.1

libjasper1-1.900.14-181.1

libjasper1-debuginfo-32bit-1.900.14-181.1

jasper-debuginfo-1.900.14-181.1

jasper-debugsource-1.900.14-181.1

libjasper1-debuginfo-1.900.14-181.1

SuSE SLES 12 SP1

x86\_64  
libjasper1-32bit-1.900.14-181.1  
libjasper1-1.900.14-181.1  
libjasper1-debuginfo-32bit-1.900.14-181.1  
jasper-debuginfo-1.900.14-181.1  
jasper-debugsource-1.900.14-181.1  
libjasper1-debuginfo-1.900.14-181.1

#### 144990 - SuSE SLED 12 SP1 SUSE-SU-2016:2778-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7857, CVE-2016-7858, CVE-2016-7859, CVE-2016-7860, CVE-2016-7861, CVE-2016-7862, CVE-2016-7863, CVE-2016-7864, CVE-2016-7865

#### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2778-1

#### 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-November/002400.html>

SuSE SLED 12 SP1  
x86\_64  
flash-player-11.2.202.644-149.1  
flash-player-gnome-11.2.202.644-149.1

#### 144991 - SuSE Linux 13.2 openSUSE-SU-2016:2769-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-3459, CVE-2016-3477, CVE-2016-3486, CVE-2016-3492, CVE-2016-3501, CVE-2016-3521, CVE-2016-3614, CVE-2016-3615, CVE-2016-5439, CVE-2016-5440, CVE-2016-5507, CVE-2016-5584, CVE-2016-5609, CVE-2016-5612, CVE-2016-5616, CVE-2016-5617, CVE-2016-5626, CVE-2016-5627, CVE-2016-5629, CVE-2016-5630, CVE-2016-6304, CVE-2016-6662, CVE-2016-7440, CVE-2016-8283, CVE-2016-8284, CVE-2016-8288

#### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2769-1

#### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00029.html>

SuSE Linux 13.2  
x86\_64  
libmysql56client18-debuginfo-5.6.34-2.23.1  
mysql-community-server-debuginfo-5.6.34-2.23.1  
mysql-community-server-tools-debuginfo-5.6.34-2.23.1  
mysql-community-server-debugsource-5.6.34-2.23.1  
libmysql56client18-debuginfo-32bit-5.6.34-2.23.1

mysql-community-server-bench-5.6.34-2.23.1  
mysql-community-server-client-5.6.34-2.23.1  
libmysql56client18-32bit-5.6.34-2.23.1  
libmysql56client18-5.6.34-2.23.1  
mysql-community-server-tools-5.6.34-2.23.1  
libmysql56client\_r18-5.6.34-2.23.1  
mysql-community-server-bench-debuginfo-5.6.34-2.23.1  
mysql-community-server-5.6.34-2.23.1  
libmysql56client\_r18-32bit-5.6.34-2.23.1  
mysql-community-server-test-5.6.34-2.23.1  
mysql-community-server-errormessages-5.6.34-2.23.1  
mysql-community-server-test-debuginfo-5.6.34-2.23.1  
mysql-community-server-client-debuginfo-5.6.34-2.23.1

i586

libmysql56client18-debuginfo-5.6.34-2.23.1  
mysql-community-server-debuginfo-5.6.34-2.23.1  
mysql-community-server-tools-debuginfo-5.6.34-2.23.1  
mysql-community-server-debugsource-5.6.34-2.23.1  
mysql-community-server-bench-5.6.34-2.23.1  
mysql-community-server-client-5.6.34-2.23.1  
libmysql56client18-5.6.34-2.23.1  
mysql-community-server-tools-5.6.34-2.23.1  
libmysql56client\_r18-5.6.34-2.23.1  
mysql-community-server-bench-debuginfo-5.6.34-2.23.1  
mysql-community-server-5.6.34-2.23.1  
mysql-community-server-test-5.6.34-2.23.1  
mysql-community-server-errormessages-5.6.34-2.23.1  
mysql-community-server-test-debuginfo-5.6.34-2.23.1  
mysql-community-server-client-debuginfo-5.6.34-2.23.1

## 144992 - SuSE SLES 11 SP4 SUSE-SU-2016:2776-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-3522, CVE-2015-5203, CVE-2015-5221, CVE-2016-1577, CVE-2016-1867, CVE-2016-2089, CVE-2016-2116, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8880, CVE-2016-8881, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2776-1

### 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-November/002399.html>

SuSE SLES 11 SP4

i586

libjasper-1.900.14-134.25.1

x86\_64

libjasper-32bit-1.900.14-134.25.1

libjasper-1.900.14-134.25.1



## 144997 - SuSE SLES 11 SP4 SUSE-SU-2016:2780-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5584, CVE-2016-6662, CVE-2016-7440

### Description

The scan detected that the host is missing the following update:  
SUSE-SU-2016:2780-1

### 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-November/002401.html>

SuSE SLES 11 SP4

i586

libmysql55client18-5.5.53-0.30.1

mysql-5.5.53-0.30.1

libmysql55client\_r18-5.5.53-0.30.1

mysql-client-5.5.53-0.30.1

mysql-tools-5.5.53-0.30.1

x86\_64

mysql-client-5.5.53-0.30.1

libmysql55client\_r18-5.5.53-0.30.1

libmysql55client18-5.5.53-0.30.1

mysql-5.5.53-0.30.1

mysql-tools-5.5.53-0.30.1

libmysql55client\_r18-32bit-5.5.53-0.30.1

libmysql55client18-32bit-5.5.53-0.30.1

## 163199 - Oracle Enterprise Linux ELSA-2016-2595 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2595

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006480.html>

OEL7

x86\_64

mariadb-embedded-devel-5.5.52-1.el7

mariadb-test-5.5.52-1.el7

mariadb-libs-5.5.52-1.el7

mariadb-embedded-5.5.52-1.el7

mariadb-server-5.5.52-1.el7  
mariadb-5.5.52-1.el7  
mariadb-bench-5.5.52-1.el7  
mariadb-devel-5.5.52-1.el7

## 163200 - Oracle Enterprise Linux ELSA-2016-2586 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2586

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006476.html>

OEL7  
x86\_64  
python-2.7.5-48.0.1.el7  
python-libs-2.7.5-48.0.1.el7  
python-debug-2.7.5-48.0.1.el7  
python-test-2.7.5-48.0.1.el7  
python-devel-2.7.5-48.0.1.el7  
python-tools-2.7.5-48.0.1.el7  
tkinter-2.7.5-48.0.1.el7

## 163218 - Oracle Enterprise Linux ELSA-2016-2574 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4312, CVE-2015-5157, CVE-2015-5307, CVE-2015-7550, CVE-2015-7872, CVE-2015-8104, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8767, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2015-8956, CVE-2016-0728, CVE-2016-0758, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2143, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3134, CVE-2016-3156, CVE-2016-3699, CVE-2016-3841, CVE-2016-4470, CVE-2016-4565, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5195, CVE-2016-5412, CVE-2016-5696, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2016-7039

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2574

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006475.html>

OEL7  
x86\_64  
kernel-headers-3.10.0-514.el7  
kernel-doc-3.10.0-514.el7

kernel-abi-whitelists-3.10.0-514.el7  
kernel-tools-3.10.0-514.el7  
python-perf-3.10.0-514.el7  
kernel-devel-3.10.0-514.el7  
kernel-tools-libs-3.10.0-514.el7  
kernel-debug-devel-3.10.0-514.el7  
kernel-tools-libs-devel-3.10.0-514.el7  
kernel-3.10.0-514.el7  
kernel-debug-3.10.0-514.el7  
perf-3.10.0-514.el7

### 182171 - FreeBSD flash Multiple Vulnerabilities (96f6bf10-a731-11e6-95ca-0011d823eebd)

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

Risk Level: High

CVE: CVE-2016-7857, CVE-2016-7858, CVE-2016-7859, CVE-2016-7860, CVE-2016-7861, CVE-2016-7862, CVE-2016-7863, CVE-2016-7864, CVE-2016-7865

#### Description

The scan detected that the host is missing the following update:  
flash -- multiple vulnerabilities (96f6bf10-a731-11e6-95ca-0011d823eebd)

#### Observation

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

<http://www.vuxml.org/freebsd/96f6bf10-a731-11e6-95ca-0011d823eebd.html>

Affected packages:

linux-c6-flashplugin < 11.2r202.644  
linux-c7-flashplugin < 11.2r202.644  
linux-f10-flashplugin < 11.2r202.644

### 185478 - Ubuntu Linux 12.04 USN-3126-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7042, CVE-2016-7117

#### Description

The scan detected that the host is missing the following update:  
USN-3126-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003623.html>

Ubuntu 12.04

linux-image-3.2.0-1493-omap4\_3.2.0-1493.120  
linux-image-omap4\_3.2.0.1493.88

### 185479 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3125-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5403, CVE-2016-6833, CVE-2016-6834, CVE-2016-6835, CVE-2016-6836, CVE-2016-6888, CVE-2016-7116, CVE-2016-7155, CVE-2016-7156, CVE-2016-7157, CVE-2016-7161, CVE-2016-7170, CVE-2016-7421, CVE-2016-7422, CVE-2016-7423, CVE-2016-7466, CVE-2016-7908, CVE-2016-7909, CVE-2016-7994, CVE-2016-7995, CVE-2016-8576, CVE-2016-8577, CVE-2016-8578, CVE-2016-8668, CVE-2016-8909, CVE-2016-8910, CVE-2016-9101, CVE-2016-9102, CVE-2016-9103, CVE-2016-9104, CVE-2016-9105, CVE-2016-9106

### Description

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

USN-3125-1

### 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-November/003621.html>

Ubuntu 12.04

qemu-kvm\_1.0+noroms-0ubuntu14.31

Ubuntu 16.04

qemu-system-s390x\_2.5+dfsg-5ubuntu10.6  
qemu-system-aarch64\_2.5+dfsg-5ubuntu10.6  
qemu-system-sparc\_2.5+dfsg-5ubuntu10.6  
qemu-system-arm\_2.5+dfsg-5ubuntu10.6  
qemu-system-ppc\_2.5+dfsg-5ubuntu10.6  
qemu-system-mips\_2.5+dfsg-5ubuntu10.6  
qemu-system\_2.5+dfsg-5ubuntu10.6  
qemu-system-misc\_2.5+dfsg-5ubuntu10.6  
qemu-system-x86\_2.5+dfsg-5ubuntu10.6

Ubuntu 14.04

qemu-system-arm\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-misc\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-ppc\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-mips\_2.0.0+dfsg-2ubuntu1.30  
qemu-system\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-sparc\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-aarch64\_2.0.0+dfsg-2ubuntu1.30  
qemu-system-x86\_2.0.0+dfsg-2ubuntu1.30

Ubuntu 16.10

qemu-system-x86\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-sparc\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-s390x\_2.6.1+dfsg-0ubuntu5.1  
qemu-system\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-aarch64\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-misc\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-arm\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-ppc\_2.6.1+dfsg-0ubuntu5.1  
qemu-system-mips\_2.6.1+dfsg-0ubuntu5.1

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

Risk Level: High

CVE: CVE-2016-7042, CVE-2016-7117

#### Description

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

USN-3126-1

#### 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-November/003622.html>

Ubuntu 12.04

linux-image-omap\_3.2.0.115.131

linux-image-powerpc64-smp\_3.2.0.115.131

linux-image-powerpc\_3.2.0.115.131

linux-image-3.2.0-115-omap\_3.2.0-115.157

linux-image-3.2.0-115-highbank\_3.2.0-115.157

linux-image-3.2.0-115-powerpc64-smp\_3.2.0-115.157

linux-image-virtual\_3.2.0.115.131

linux-image-generic-pae\_3.2.0.115.131

linux-image-highbank\_3.2.0.115.131

linux-image-3.2.0-115-generic-pae\_3.2.0-115.157

linux-image-generic\_3.2.0.115.131

linux-image-powerpc-smp\_3.2.0.115.131

linux-image-3.2.0-115-virtual\_3.2.0-115.157

linux-image-3.2.0-115-generic\_3.2.0-115.157

linux-image-3.2.0-115-powerpc-smp\_3.2.0-115.157

## 20721 - Cisco NX-OS Software Authentication Authorization Accounting Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-0721

#### Description

A vulnerability is present in some versions of Cisco NX-OS.

#### Observation

Cisco NX-OS Software is an operating system used in Cisco Nexus devices.

A vulnerability is present in some versions of Cisco NX-OS. The flaw lies in the SSH subsystem. Successful exploitation could allow an attacker to bypass security access restrictions.

## 20851 - (HT207275) Apple OS X Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-4660, CVE-2016-4661, CVE-2016-4662, CVE-2016-4663, CVE-2016-4667, CVE-2016-4669, CVE-2016-4670, CVE-2016-4671, CVE-2016-4673, CVE-2016-4674, CVE-2016-4675, CVE-2016-4678, CVE-2016-4679, CVE-2016-4681, CVE-2016-4682, CVE-2016-4683, CVE-2016-4721, CVE-2016-7577, CVE-2016-7579, CVE-2016-7613

### Description

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

### Observation

Apple OS X is an operating system used in Apple computers.

Multiple vulnerabilities are present in some versions of Apple OS X. The flaws lie in multiple components. Successful exploitation could allow an attacker to gain elevated user privileges, obtain sensitive information, cause denial of service or execute arbitrary code.

## **20858 - (HT207273) Apple iCloud WebKit Multiple Vulnerabilities Prior To 6.0.1**

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

Risk Level: High

CVE: CVE-2016-4613, CVE-2016-7578

### Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

### Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

Multiple vulnerabilities are present in some versions of Apple iCloud. The flaws lie in webkit component. Successful exploitation could allow an attacker to retrieve sensitive data or execute arbitrary code.

## **20865 - (MS11-016) Microsoft Groove Insecure Library Loading RCE (2494047)**

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

Risk Level: High

CVE: CVE-2010-3146

### Description

A remote code execution vulnerability is present in some versions of Microsoft Office Groove.

### Observation

Microsoft Office Groove is a software used for team projects collaboration.

A remote code execution vulnerability is present in some versions of Microsoft Office Groove. The flaw is due to how this product handles the DLL files loading process. Successful exploitation could allow an attacker to escalate privileges or execute arbitrary code.

Microsoft has provided MS11-016 to address this issue. The host appears to be missing this patch.

## **20868 - Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPSR)**

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

Risk Level: High

CVE: CVE-2016-0772, CVE-2016-5636, CVE-2016-5699

### Description

Multiple vulnerabilities are present in some versions of Splunk Enterprise.

## Observation

Splunk Enterprise is an operational intelligence solution

Multiple vulnerabilities are present in some versions of Splunk Enterprise. The flaws lie in multiple components. Successful exploitation by a remote attacker could lead to obtain sensitive information, cause denial of service or execute arbitrary code.

### **20876 - Novell iPrint Appliance Multiple Vulnerabilities Prior To 2.0 Patch 3**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-2015, CVE-2013-3009, CVE-2013-4312, CVE-2013-5456, CVE-2013-5653, CVE-2013-7446, CVE-2014-3566, CVE-2014-9767, CVE-2015-0272, CVE-2015-0293, CVE-2015-3195, CVE-2015-3197, CVE-2015-3228, CVE-2015-4116, CVE-2015-5041, CVE-2015-5194, CVE-2015-5219, CVE-2015-5300, CVE-2015-5370, CVE-2015-7509, CVE-2015-7513, CVE-2015-7550, CVE-2015-7566, CVE-2015-7575, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7799, CVE-2015-7803, CVE-2015-7833, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855, CVE-2015-7871, CVE-2015-7973, CVE-2015-7974, CVE-2015-7976, CVE-2015-7978, CVE-2015-7979, CVE-2015-7981, CVE-2015-8126, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158, CVE-2015-8215, CVE-2015-8325, CVE-2015-8472, CVE-2015-8539, CVE-2015-8540, CVE-2015-8543, CVE-2015-8550, CVE-2015-8551, CVE-2015-8552, CVE-2015-8569, CVE-2015-8575, CVE-2015-8767, CVE-2015-8785, CVE-2015-8806, CVE-2015-8812, CVE-2015-8816, CVE-2015-8835, CVE-2015-8838, CVE-2015-8866, CVE-2015-8867, CVE-2015-8873, CVE-2015-8874, CVE-2015-8879, CVE-2016-0264, CVE-2016-0363, CVE-2016-0376, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0483, CVE-2016-0494, CVE-2016-0686, CVE-2016-0687, CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-0705, CVE-2016-0723, CVE-2016-0758, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800

## Description

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance.

## Observation

Novell iPrint Appliance is a popular virtual appliance that offers self-service printing for the enterprises.

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code, bypass security measures or cause a denial of service condition.

### **160167 - CentOS 6 CESA-2016-2658 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

## Description

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

CESA-2016-2658

## Observation

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

For more information see:

<http://lists.centos.org/pipermail/centos-announce/2016-November/022140.html>

CentOS 6

i686

java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6\_8

java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6\_8

java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6\_8

java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6\_8

noarch  
java-1.7.0-openjdk-javadoc-1.7.0.121-2.6.8.1.el6\_8

x86\_64  
java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6\_8  
java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6\_8  
java-1.7.0-openjdk-demo-1.7.0.121-2.6.8.1.el6\_8  
java-1.7.0-openjdk-src-1.7.0.121-2.6.8.1.el6\_8

## 163205 - Oracle Enterprise Linux ELSA-2016-2579 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0794, CVE-2016-0795, CVE-2016-4324

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2579

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006467.html>

OEL7  
x86\_64  
libreoffice-langpack-nso-5.0.6.2-3.0.1.el7  
libreoffice-5.0.6.2-3.0.1.el7  
autocorr-ja-5.0.6.2-3.0.1.el7  
libcmis-devel-0.5.1-2.el7  
libreoffice-langpack-gu-5.0.6.2-3.0.1.el7  
libreoffice-nlpsolver-5.0.6.2-3.0.1.el7  
libreoffice-langpack-zh-Hant-5.0.6.2-3.0.1.el7  
libreoffice-langpack-fa-5.0.6.2-3.0.1.el7  
libreoffice-langpack-or-5.0.6.2-3.0.1.el7  
libreoffice-langpack-hu-5.0.6.2-3.0.1.el7  
libreoffice-langpack-pa-5.0.6.2-3.0.1.el7  
autocorr-de-5.0.6.2-3.0.1.el7  
libreoffice-langpack-xh-5.0.6.2-3.0.1.el7  
libreoffice-ure-5.0.6.2-3.0.1.el7  
autocorr-sv-5.0.6.2-3.0.1.el7  
libreoffice-langpack-fr-5.0.6.2-3.0.1.el7  
libreoffice-langpack-as-5.0.6.2-3.0.1.el7  
libreoffice-langpack-nn-5.0.6.2-3.0.1.el7  
libreoffice-langpack-bn-5.0.6.2-3.0.1.el7  
libreoffice-librelogo-5.0.6.2-3.0.1.el7  
libreoffice-langpack-zu-5.0.6.2-3.0.1.el7  
autocorr-pt-5.0.6.2-3.0.1.el7  
libreoffice-langpack-tn-5.0.6.2-3.0.1.el7  
libreoffice-langpack-br-5.0.6.2-3.0.1.el7  
autocorr-en-5.0.6.2-3.0.1.el7  
libreoffice-langpack-sv-5.0.6.2-3.0.1.el7  
libreoffice-langpack-el-5.0.6.2-3.0.1.el7  
autocorr-lb-5.0.6.2-3.0.1.el7  
libreoffice-math-5.0.6.2-3.0.1.el7  
autocorr-it-5.0.6.2-3.0.1.el7  
libreoffice-langpack-si-5.0.6.2-3.0.1.el7



libreoffice-langpack-ml-5.0.6.2-3.0.1.el7  
libpagemaker-tools-0.0.3-1.el7  
autocorr-vi-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ru-5.0.6.2-3.0.1.el7  
libpagemaker-doc-0.0.3-1.el7  
libreoffice-langpack-da-5.0.6.2-3.0.1.el7  
libreoffice-sdk-doc-5.0.6.2-3.0.1.el7  
libreoffice-langpack-te-5.0.6.2-3.0.1.el7  
libreoffice-langpack-cy-5.0.6.2-3.0.1.el7  
libreoffice-langpack-it-5.0.6.2-3.0.1.el7  
libreoffice-rhino-5.0.6.2-3.0.1.el7  
libreoffice-langpack-zh-Hans-5.0.6.2-3.0.1.el7  
autocorr-sk-5.0.6.2-3.0.1.el7  
autocorr-bg-5.0.6.2-3.0.1.el7  
libreoffice-base-5.0.6.2-3.0.1.el7  
libreoffice-opensymbol-fonts-5.0.6.2-3.0.1.el7  
libreoffice-calc-5.0.6.2-3.0.1.el7  
autocorr-ca-5.0.6.2-3.0.1.el7  
autocorr-fi-5.0.6.2-3.0.1.el7  
autocorr-ru-5.0.6.2-3.0.1.el7  
libreoffice-langpack-sk-5.0.6.2-3.0.1.el7  
autocorr-ro-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ar-5.0.6.2-3.0.1.el7  
libreoffice-langpack-th-5.0.6.2-3.0.1.el7  
libreoffice-langpack-st-5.0.6.2-3.0.1.el7  
libreoffice-langpack-fi-5.0.6.2-3.0.1.el7  
libreoffice-langpack-eu-5.0.6.2-3.0.1.el7  
autocorr-hu-5.0.6.2-3.0.1.el7  
libreoffice-postgresql-5.0.6.2-3.0.1.el7  
libreoffice-langpack-nr-5.0.6.2-3.0.1.el7  
libreoffice-langpack-bg-5.0.6.2-3.0.1.el7  
libreoffice-langpack-uk-5.0.6.2-3.0.1.el7  
libreoffice-langpack-lv-5.0.6.2-3.0.1.el7  
libreoffice-writer-5.0.6.2-3.0.1.el7  
libreoffice-langpack-hi-5.0.6.2-3.0.1.el7  
libreoffice-graphicfilter-5.0.6.2-3.0.1.el7  
autocorr-af-5.0.6.2-3.0.1.el7  
autocorr-pl-5.0.6.2-3.0.1.el7  
autocorr-mn-5.0.6.2-3.0.1.el7  
libreoffice-langpack-nl-5.0.6.2-3.0.1.el7  
autocorr-ko-5.0.6.2-3.0.1.el7  
libreoffice-langpack-cs-5.0.6.2-3.0.1.el7  
libreoffice-officebean-5.0.6.2-3.0.1.el7  
libreoffice-core-5.0.6.2-3.0.1.el7  
libreoffice-langpack-kk-5.0.6.2-3.0.1.el7  
libreoffice-langpack-he-5.0.6.2-3.0.1.el7  
autocorr-sl-5.0.6.2-3.0.1.el7  
autocorr-sr-5.0.6.2-3.0.1.el7  
libreoffice-langpack-mr-5.0.6.2-3.0.1.el7  
autocorr-da-5.0.6.2-3.0.1.el7  
libreoffice-langpack-gl-5.0.6.2-3.0.1.el7  
libreoffice-filters-5.0.6.2-3.0.1.el7  
autocorr-tr-5.0.6.2-3.0.1.el7  
libreoffice-wiki-publisher-5.0.6.2-3.0.1.el7  
libreoffice-langpack-kn-5.0.6.2-3.0.1.el7  
libreoffice-draw-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ve-5.0.6.2-3.0.1.el7  
autocorr-ga-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ga-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ts-5.0.6.2-3.0.1.el7

autocorr-zh-5.0.6.2-3.0.1.el7  
libreoffice-langpack-nb-5.0.6.2-3.0.1.el7  
libreoffice-impress-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ca-5.0.6.2-3.0.1.el7  
libpagemaker-0.0.3-1.el7  
libreoffice-sdk-5.0.6.2-3.0.1.el7  
libreoffice-langpack-lt-5.0.6.2-3.0.1.el7  
libreoffice-langpack-et-5.0.6.2-3.0.1.el7  
libreoffice-langpack-sr-5.0.6.2-3.0.1.el7  
libreoffice-pdfimport-5.0.6.2-3.0.1.el7  
libreoffice-langpack-af-5.0.6.2-3.0.1.el7  
libreoffice-gdb-debug-support-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ro-5.0.6.2-3.0.1.el7  
libpagemaker-devel-0.0.3-1.el7  
libreoffice-pyuno-5.0.6.2-3.0.1.el7  
libreoffice-ogltrans-5.0.6.2-3.0.1.el7  
autocorr-fr-5.0.6.2-3.0.1.el7  
libreoffice-xsltfilter-5.0.6.2-3.0.1.el7  
libreoffice-langpack-pt-PT-5.0.6.2-3.0.1.el7  
autocorr-cs-5.0.6.2-3.0.1.el7  
libreoffice-glade-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ta-5.0.6.2-3.0.1.el7  
libreoffice-bsh-5.0.6.2-3.0.1.el7  
autocorr-nl-5.0.6.2-3.0.1.el7  
libcmis-tools-0.5.1-2.el7  
libreoffice-emailmerge-5.0.6.2-3.0.1.el7  
libreoffice-langpack-es-5.0.6.2-3.0.1.el7  
libreoffice-langpack-pl-5.0.6.2-3.0.1.el7  
libcmis-0.5.1-2.el7  
libreoffice-langpack-mai-5.0.6.2-3.0.1.el7  
autocorr-lt-5.0.6.2-3.0.1.el7  
libreoffice-langpack-pt-BR-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ko-5.0.6.2-3.0.1.el7  
mdds-devel-0.12.1-1.el7  
libreoffice-langpack-ja-5.0.6.2-3.0.1.el7  
libreoffice-langpack-tr-5.0.6.2-3.0.1.el7  
libreoffice-langpack-hr-5.0.6.2-3.0.1.el7  
autocorr-es-5.0.6.2-3.0.1.el7  
libreoffice-langpack-en-5.0.6.2-3.0.1.el7  
libreoffice-langpack-de-5.0.6.2-3.0.1.el7  
autocorr-fa-5.0.6.2-3.0.1.el7  
libreoffice-langpack-ss-5.0.6.2-3.0.1.el7  
libreoffice-langpack-sl-5.0.6.2-3.0.1.el7  
autocorr-is-5.0.6.2-3.0.1.el7  
libreoffice-langpack-dz-5.0.6.2-3.0.1.el7  
autocorr-hr-5.0.6.2-3.0.1.el7

## 163209 - Oracle Enterprise Linux ELSA-2016-2580 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2580

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006470.html>

OEL7

x86\_64

poppler-qt-devel-0.26.5-16.el7

poppler-qt-0.26.5-16.el7

poppler-0.26.5-16.el7

poppler-devel-0.26.5-16.el7

poppler-cpp-devel-0.26.5-16.el7

poppler-demos-0.26.5-16.el7

poppler-cpp-0.26.5-16.el7

poppler-glib-devel-0.26.5-16.el7

poppler-glib-0.26.5-16.el7

poppler-utils-0.26.5-16.el7

### 163217 - Oracle Enterprise Linux ELSA-2016-2587 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-4877, CVE-2016-4971

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2587

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006485.html>

OEL7

x86\_64

wget-1.14-13.el7

### 178239 - Gentoo Linux GLSA-201611-08 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7981, CVE-2015-8126, CVE-2015-8540

#### Description

The scan detected that the host is missing the following update:  
GLSA-201611-08

#### Observation

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

<https://security.gentoo.org/glsa/201611-08>

Affected packages:

media-libs/libpng < 1.6.21

## 20869 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.98

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

Risk Level: High

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202

### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

### Observation

Google Chrome is a popular Internet browser.

Multiple vulnerabilities are present in some versions of Google Chrome. These flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service, obtain sensitive information, or execute arbitrary code.

## 20870 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.98

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202

### Description

Multiple vulnerabilities are present in some versions of Google Chrome.

### Observation

Google Chrome is a popular Internet browser.

Multiple vulnerabilities are present in some versions of Google Chrome. These flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service, obtain sensitive information, or execute arbitrary code.

## 20859 - (SOL01276005) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-2182

### 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 vulnerability lies in some versions of the OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition.

## 20860 - Joomla Multiple Vulnerabilities Prior To 3.6.4

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

Risk Level: High

CVE: CVE-2016-8869, CVE-2016-8870, CVE-2016-9081

### Description

Multiple vulnerabilities are present in some versions of Joomla!.

### Observation

Joomla! Is a popular content management system.

Multiple vulnerabilities are present in some versions of Joomla!. The flaws lie in several components. Successful exploitation could allow an attacker to modify existing user accounts, register on a site with elevated privileges or even when registration has been disabled.

## **20866 - (HPSBUX03665) HP-UX Tomcat-based Servlet Engine Denial Of Service And URL Redirection Vulnerabilities**

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-3092, CVE-2016-5388

### Description

Multiple vulnerabilities are present in some versions of HP-UX.

### Observation

HP-UX is a Unix-like operating system.

Multiple vulnerabilities are present in some versions of HP-UX. The flaws lie in Tomcat-based Servlet Engine. Successful exploitation could allow an attacker to cause denial of service or URL redirection.

## **132298 - Oracle VM OVMSA-2016-0157 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-7545

### Description

The scan detected that the host is missing the following update:  
OVMSA-2016-0157

### Observation

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

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000581.html>

<http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000580.html>

OVM3.3

x86\_64

policycoreutils-2.0.83-30.1.0.1.el6\_8

OVM3.4

x86\_64

policycoreutils-2.0.83-30.1.0.1.el6\_8

## **141363 - Red Hat Enterprise Linux RHSA-2016-2766 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-2143

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2766

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2766.html>

#### RHEL6D

i386  
kernel-headers-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6  
kernel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6

#### noarch

kernel-firmware-2.6.32-642.11.1.el6  
kernel-doc-2.6.32-642.11.1.el6  
kernel-abi-whitelists-2.6.32-642.11.1.el6

#### x86\_64

kernel-2.6.32-642.11.1.el6  
kernel-headers-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6

#### RHEL6S

i386  
kernel-headers-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6

kernel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6

noarch  
kernel-firmware-2.6.32-642.11.1.el6  
kernel-doc-2.6.32-642.11.1.el6  
kernel-abi-whitelists-2.6.32-642.11.1.el6

x86\_64  
kernel-2.6.32-642.11.1.el6  
kernel-headers-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6

## RHEL6WS

i386  
kernel-headers-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6  
kernel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6

noarch  
kernel-firmware-2.6.32-642.11.1.el6  
kernel-doc-2.6.32-642.11.1.el6  
kernel-abi-whitelists-2.6.32-642.11.1.el6

x86\_64  
kernel-headers-2.6.32-642.11.1.el6  
python-perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
perf-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-2.6.32-642.11.1.el6  
kernel-debuginfo-common-x86\_64-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-debuginfo-common-i686-2.6.32-642.11.1.el6  
kernel-2.6.32-642.11.1.el6  
kernel-debug-debuginfo-2.6.32-642.11.1.el6

## 141365 - Red Hat Enterprise Linux RHSA-2016-2702 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2702

### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2702.html>

#### RHEL6S

i386

polycycoreutils-2.0.83-30.1.el6\_8  
polycycoreutils-newrole-2.0.83-30.1.el6\_8  
polycycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycycoreutils-gui-2.0.83-30.1.el6\_8  
polycycoreutils-python-2.0.83-30.1.el6\_8

x86\_64

polycycoreutils-2.0.83-30.1.el6\_8  
polycycoreutils-newrole-2.0.83-30.1.el6\_8  
polycycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycycoreutils-gui-2.0.83-30.1.el6\_8  
polycycoreutils-python-2.0.83-30.1.el6\_8

#### RHEL6WS

x86\_64

polycycoreutils-2.0.83-30.1.el6\_8  
polycycoreutils-newrole-2.0.83-30.1.el6\_8  
polycycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycycoreutils-gui-2.0.83-30.1.el6\_8  
polycycoreutils-python-2.0.83-30.1.el6\_8

i386

polycycoreutils-2.0.83-30.1.el6\_8  
polycycoreutils-newrole-2.0.83-30.1.el6\_8  
polycycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycycoreutils-gui-2.0.83-30.1.el6\_8  
polycycoreutils-python-2.0.83-30.1.el6\_8

#### RHEL7D

x86\_64

polycycoreutils-2.5-9.el7  
polycycoreutils-devel-2.5-9.el7  
polycycoreutils-gui-2.5-9.el7  
polycycoreutils-newrole-2.5-9.el7  
polycycoreutils-debuginfo-2.5-9.el7  
polycycoreutils-python-2.5-9.el7  
polycycoreutils-restorecond-2.5-9.el7  
polycycoreutils-sandbox-2.5-9.el7

#### RHEL6D

x86\_64



polycoreutils-2.0.83-30.1.el6\_8  
polycoreutils-newrole-2.0.83-30.1.el6\_8  
polycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycoreutils-gui-2.0.83-30.1.el6\_8  
polycoreutils-python-2.0.83-30.1.el6\_8

i386

polycoreutils-2.0.83-30.1.el6\_8  
polycoreutils-newrole-2.0.83-30.1.el6\_8  
polycoreutils-sandbox-2.0.83-30.1.el6\_8  
polycoreutils-debuginfo-2.0.83-30.1.el6\_8  
polycoreutils-gui-2.0.83-30.1.el6\_8  
polycoreutils-python-2.0.83-30.1.el6\_8

RHEL7WS

x86\_64  
polycoreutils-2.5-9.el7  
polycoreutils-devel-2.5-9.el7  
polycoreutils-gui-2.5-9.el7  
polycoreutils-newrole-2.5-9.el7  
polycoreutils-debuginfo-2.5-9.el7  
polycoreutils-python-2.5-9.el7  
polycoreutils-restorecond-2.5-9.el7  
polycoreutils-sandbox-2.5-9.el7

## 141366 - Red Hat Enterprise Linux RHSA-2016-2718 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202

### Description

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

RHSA-2016-2718

### Observation

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

For more information see:

<https://rhn.redhat.com/errata/RHSA-2016-2718.html>

RHEL6D

x86\_64  
chromium-browser-debuginfo-54.0.2840.100-1.el6  
chromium-browser-54.0.2840.100-1.el6

i386

chromium-browser-debuginfo-54.0.2840.100-1.el6  
chromium-browser-54.0.2840.100-1.el6

RHEL6S

x86\_64  
chromium-browser-debuginfo-54.0.2840.100-1.el6  
chromium-browser-54.0.2840.100-1.el6

i386

chromium-browser-debuginfo-54.0.2840.100-1.el6

chromium-browser-54.0.2840.100-1.el6

RHEL6WS

x86\_64

chromium-browser-debuginfo-54.0.2840.100-1.el6

chromium-browser-54.0.2840.100-1.el6

i386

chromium-browser-debuginfo-54.0.2840.100-1.el6

chromium-browser-54.0.2840.100-1.el6

## 144993 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2764-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5011

### Description

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

SUSE-SU-2016:2764-1

### 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-November/002396.html>

SuSE SLES 12 SP1

noarch

util-linux-lang-2.25-37.1

x86\_64

libblkid1-debuginfo-2.25-37.1

libmount1-debuginfo-32bit-2.25-37.1

libmount1-2.25-37.1

util-linux-2.25-37.1

uuidd-debuginfo-2.25-37.1

libuuid1-2.25-37.1

python-libmount-debugsource-2.25-37.1

util-linux-debugsource-2.25-37.1

libuuid1-32bit-2.25-37.1

libblkid1-32bit-2.25-37.1

libblkid1-debuginfo-32bit-2.25-37.1

libsmartcols1-2.25-37.1

util-linux-systemd-2.25-37.1

libmount1-32bit-2.25-37.1

python-libmount-2.25-37.1

uuidd-2.25-37.1

util-linux-systemd-debugsource-2.25-37.1

libuuid1-debuginfo-32bit-2.25-37.1

libblkid1-2.25-37.1

python-libmount-debuginfo-2.25-37.1

libmount1-debuginfo-2.25-37.1

libsmartcols1-debuginfo-2.25-37.1

libuuid1-debuginfo-2.25-37.1

util-linux-debuginfo-2.25-37.1

util-linux-systemd-debuginfo-2.25-37.1

SuSE SLED 12 SP1  
x86\_64  
libblkid1-debuginfo-2.25-37.1  
libmount1-debuginfo-32bit-2.25-37.1  
libmount1-2.25-37.1  
libuuid-devel-2.25-37.1  
util-linux-2.25-37.1  
libuuid1-32bit-2.25-37.1  
libuuid1-2.25-37.1  
python-libmount-debuginfo-2.25-37.1  
util-linux-debugsource-2.25-37.1  
uuidd-debuginfo-2.25-37.1  
python-libmount-debugsource-2.25-37.1  
libblkid1-32bit-2.25-37.1  
libblkid1-debuginfo-32bit-2.25-37.1  
libsmartcols1-2.25-37.1  
util-linux-systemd-2.25-37.1  
libmount1-32bit-2.25-37.1  
libsmartcols1-debuginfo-2.25-37.1  
python-libmount-2.25-37.1  
uuidd-2.25-37.1  
util-linux-systemd-debugsource-2.25-37.1  
libuuid1-debuginfo-32bit-2.25-37.1  
libmount1-debuginfo-2.25-37.1  
libblkid1-2.25-37.1  
libuuid1-debuginfo-2.25-37.1  
util-linux-debuginfo-2.25-37.1  
util-linux-systemd-debuginfo-2.25-37.1

noarch  
util-linux-lang-2.25-37.1

## 144994 - SuSE Linux 13.2 openSUSE-SU-2016:2793-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2793-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00045.html>

SuSE Linux 13.2  
x86\_64  
chromium-ffmpegsumo-debuginfo-54.0.2840.100-140.1  
chromium-54.0.2840.100-140.1  
chromium-debuginfo-54.0.2840.100-140.1  
chromedriver-debuginfo-54.0.2840.100-140.1  
chromedriver-54.0.2840.100-140.1  
chromium-ffmpegsumo-54.0.2840.100-140.1  
chromium-debugsource-54.0.2840.100-140.1

i586  
chromium-ffmpegsumo-debuginfo-54.0.2840.100-140.1  
chromium-54.0.2840.100-140.1  
chromium-debuginfo-54.0.2840.100-140.1  
chromedriver-debuginfo-54.0.2840.100-140.1  
chromedriver-54.0.2840.100-140.1  
chromium-ffmpegsumo-54.0.2840.100-140.1  
chromium-debugsource-54.0.2840.100-140.1

## 144995 - SuSE Linux 13.2 openSUSE-SU-2016:2805-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3210, CVE-2015-3217, CVE-2015-5073, CVE-2015-8380, CVE-2016-1283, CVE-2016-3191

### Description

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

openSUSE-SU-2016:2805-1

### Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00055.html>

SuSE Linux 13.2

i586  
pcre-debugsource-8.39-3.8.1  
pcre-devel-8.39-3.8.1  
libpcre16-0-8.39-3.8.1  
libpcrecpp0-debuginfo-8.39-3.8.1  
pcre-tools-8.39-3.8.1  
libpcre16-0-debuginfo-8.39-3.8.1  
pcre-devel-static-8.39-3.8.1  
pcre-tools-debuginfo-8.39-3.8.1  
libpcreposix0-debuginfo-8.39-3.8.1  
libpcrecpp0-8.39-3.8.1  
libpcre1-debuginfo-8.39-3.8.1  
libpcreposix0-8.39-3.8.1  
libpcre1-8.39-3.8.1

noarch  
pcre-doc-8.39-3.8.1

x86\_64  
libpcre1-32bit-8.39-3.8.1  
pcre-debugsource-8.39-3.8.1  
pcre-devel-8.39-3.8.1  
libpcre16-0-8.39-3.8.1  
libpcrecpp0-debuginfo-32bit-8.39-3.8.1  
libpcre16-0-32bit-8.39-3.8.1  
libpcrecpp0-debuginfo-8.39-3.8.1  
pcre-tools-8.39-3.8.1  
libpcre16-0-debuginfo-8.39-3.8.1  
libpcre1-debuginfo-32bit-8.39-3.8.1  
libpcrecpp0-32bit-8.39-3.8.1  
pcre-devel-static-8.39-3.8.1  
pcre-tools-debuginfo-8.39-3.8.1

libpcreposix0-debuginfo-8.39-3.8.1  
libpcreposix0-32bit-8.39-3.8.1  
libpcrecpp0-8.39-3.8.1  
libpcre1-debuginfo-8.39-3.8.1  
libpcre16-0-debuginfo-32bit-8.39-3.8.1  
libpcreposix0-debuginfo-32bit-8.39-3.8.1  
libpcreposix0-8.39-3.8.1  
libpcre1-8.39-3.8.1

## 144996 - SuSE Linux 13.2 openSUSE-SU-2016:2752-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5180

### Description

The scan detected that the host is missing the following update:  
openSUSE-SU-2016:2752-1

### Observation

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

<http://lists.opensuse.org/opensuse-updates/2016-11/msg00024.html>

SuSE Linux 13.2  
i586  
nodejs-4.6.1-27.1  
nodejs-devel-4.6.1-27.1  
nodejs-debuginfo-4.6.1-27.1  
nodejs-debugsource-4.6.1-27.1

noarch  
nodejs-doc-4.6.1-27.1

x86\_64  
nodejs-4.6.1-27.1  
nodejs-devel-4.6.1-27.1  
nodejs-debuginfo-4.6.1-27.1  
nodejs-debugsource-4.6.1-27.1

## 160165 - CentOS 6 CESA-2016-2675 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7035

### Description

The scan detected that the host is missing the following update:  
CESA-2016-2675

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-November/022142.html>

CentOS 6

x86\_64

pacemaker-libs-1.1.14-8.el6\_8.2

pacemaker-1.1.14-8.el6\_8.2

pacemaker-libs-devel-1.1.14-8.el6\_8.2

pacemaker-doc-1.1.14-8.el6\_8.2

pacemaker-cli-1.1.14-8.el6\_8.2

pacemaker-remote-1.1.14-8.el6\_8.2

pacemaker-cluster-libs-1.1.14-8.el6\_8.2

pacemaker-cts-1.1.14-8.el6\_8.2

i686

pacemaker-libs-1.1.14-8.el6\_8.2

pacemaker-1.1.14-8.el6\_8.2

pacemaker-libs-devel-1.1.14-8.el6\_8.2

pacemaker-doc-1.1.14-8.el6\_8.2

pacemaker-cli-1.1.14-8.el6\_8.2

pacemaker-remote-1.1.14-8.el6\_8.2

pacemaker-cluster-libs-1.1.14-8.el6\_8.2

pacemaker-cts-1.1.14-8.el6\_8.2

## 163195 - Oracle Enterprise Linux ELSA-2016-2598 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5385, CVE-2016-5399, CVE-2016-5766, CVE-2016-5767, CVE-2016-5768

### Description

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

ELSA-2016-2598

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006482.html>

OEL7

x86\_64

php-bcmath-5.4.16-42.el7

php-devel-5.4.16-42.el7

php-odbc-5.4.16-42.el7

php-intl-5.4.16-42.el7

php-xml-5.4.16-42.el7

php-recode-5.4.16-42.el7

php-pdo-5.4.16-42.el7

php-embedded-5.4.16-42.el7

php-pspell-5.4.16-42.el7

php-snmp-5.4.16-42.el7

php-enchant-5.4.16-42.el7

php-ldap-5.4.16-42.el7

php-soap-5.4.16-42.el7

php-dba-5.4.16-42.el7

php-5.4.16-42.el7

php-gd-5.4.16-42.el7

php-cli-5.4.16-42.el7

php-mysqlnd-5.4.16-42.el7

php-mbstring-5.4.16-42.el7  
php-fpm-5.4.16-42.el7  
php-common-5.4.16-42.el7  
php-xmlrpc-5.4.16-42.el7  
php-pgsql-5.4.16-42.el7  
php-mysql-5.4.16-42.el7  
php-process-5.4.16-42.el7

### 163196 - Oracle Enterprise Linux ELSA-2016-2588 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2588

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006486.html>

OEL7  
x86\_64  
openssh-server-sysvinit-6.6.1p1-31.el7  
openssh-clients-6.6.1p1-31.el7  
openssh-askpass-6.6.1p1-31.el7  
openssh-server-6.6.1p1-31.el7  
openssh-keycat-6.6.1p1-31.el7  
openssh-6.6.1p1-31.el7  
pam\_ssh\_agent\_auth-0.9.3-9.31.el7  
openssh-ldap-6.6.1p1-31.el7

### 163201 - Oracle Enterprise Linux ELSA-2016-2702 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2702

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006508.html>  
<http://oss.oracle.com/pipermail/el-errata/2016-November/006507.html>

OEL7  
x86\_64  
policycoreutils-restorecond-2.5-9.0.1.el7  
policycoreutils-devel-2.5-9.0.1.el7

polycoreutils-python-2.5-9.0.1.el7  
polycoreutils-newrole-2.5-9.0.1.el7  
polycoreutils-2.5-9.0.1.el7  
polycoreutils-sandbox-2.5-9.0.1.el7  
polycoreutils-gui-2.5-9.0.1.el7

#### OEL6

x86\_64  
polycoreutils-sandbox-2.0.83-30.1.0.1.el6\_8  
polycoreutils-python-2.0.83-30.1.0.1.el6\_8  
polycoreutils-gui-2.0.83-30.1.0.1.el6\_8  
polycoreutils-newrole-2.0.83-30.1.0.1.el6\_8  
polycoreutils-2.0.83-30.1.0.1.el6\_8

#### i386

polycoreutils-sandbox-2.0.83-30.1.0.1.el6\_8  
polycoreutils-python-2.0.83-30.1.0.1.el6\_8  
polycoreutils-gui-2.0.83-30.1.0.1.el6\_8  
polycoreutils-newrole-2.0.83-30.1.0.1.el6\_8  
polycoreutils-2.0.83-30.1.0.1.el6\_8

### 163206 - Oracle Enterprise Linux ELSA-2016-2599 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7810, CVE-2015-5174, CVE-2015-5345, CVE-2015-5346, CVE-2015-5351, CVE-2016-0706, CVE-2016-0714, CVE-2016-0763, CVE-2016-3092

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2599

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006483.html>

#### OEL7

x86\_64  
tomcat-webapps-7.0.69-10.el7  
tomcat-jsvc-7.0.69-10.el7  
tomcat-docs-webapp-7.0.69-10.el7  
tomcat-7.0.69-10.el7  
tomcat-jsp-2.2-api-7.0.69-10.el7  
tomcat-admin-webapps-7.0.69-10.el7  
tomcat-el-2.2-api-7.0.69-10.el7  
tomcat-lib-7.0.69-10.el7  
tomcat-javadoc-7.0.69-10.el7  
tomcat-servlet-3.0-api-7.0.69-10.el7

### 163208 - Oracle Enterprise Linux ELSA-2016-2590 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2774



### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2590

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006478.html>

OEL7  
x86\_64  
dhcp-libs-4.2.5-47.0.1.el7  
dhcp-devel-4.2.5-47.0.1.el7  
dhcp-4.2.5-47.0.1.el7  
dhcp-common-4.2.5-47.0.1.el7  
dhclient-4.2.5-47.0.1.el7

## 163211 - Oracle Enterprise Linux ELSA-2016-2585 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1714, CVE-2016-1981, CVE-2016-3710, CVE-2016-3712, CVE-2016-5126, CVE-2016-5403

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2585

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006474.html>

OEL7  
x86\_64  
qemu-kvm-1.5.3-126.el7  
qemu-img-1.5.3-126.el7  
qemu-kvm-tools-1.5.3-126.el7  
qemu-kvm-common-1.5.3-126.el7

## 163212 - Oracle Enterprise Linux ELSA-2016-2604 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7050

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2604

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006495.html>

OEL7

x86\_64

reestasy-base-jaxrs-api-3.0.6-4.el7  
reestasy-base-tjws-3.0.6-4.el7  
reestasy-base-javadoc-3.0.6-4.el7  
reestasy-base-jaxrs-all-3.0.6-4.el7  
reestasy-base-jettison-provider-3.0.6-4.el7  
reestasy-base-providers-pom-3.0.6-4.el7  
reestasy-base-atom-provider-3.0.6-4.el7  
reestasy-base-client-3.0.6-4.el7  
reestasy-base-jaxb-provider-3.0.6-4.el7  
reestasy-base-3.0.6-4.el7  
reestasy-base-jaxrs-3.0.6-4.el7  
reestasy-base-jackson-provider-3.0.6-4.el7  
reestasy-base-reestasy-pom-3.0.6-4.el7

### 163213 - Oracle Enterprise Linux ELSA-2016-2766 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-2143, CVE-2016-5195

#### Description

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

ELSA-2016-2766

#### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006512.html>

OEL6

x86\_64

kernel-headers-2.6.32-642.11.1.el6  
kernel-doc-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-firmware-2.6.32-642.11.1.el6  
kernel-2.6.32-642.11.1.el6  
kernel-abi-whitelists-2.6.32-642.11.1.el6

i386

kernel-headers-2.6.32-642.11.1.el6  
kernel-doc-2.6.32-642.11.1.el6  
kernel-debug-2.6.32-642.11.1.el6  
kernel-debug-devel-2.6.32-642.11.1.el6  
perf-2.6.32-642.11.1.el6  
python-perf-2.6.32-642.11.1.el6  
kernel-devel-2.6.32-642.11.1.el6  
kernel-firmware-2.6.32-642.11.1.el6  
kernel-2.6.32-642.11.1.el6  
kernel-abi-whitelists-2.6.32-642.11.1.el6

## 163214 - Oracle Enterprise Linux ELSA-2016-2582 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8803, CVE-2015-8804, CVE-2015-8805, CVE-2016-6489

### Description

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

ELSA-2016-2582

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006471.html>

OEL7

x86\_64

nettle-devel-2.7.1-8.el7

nettle-2.7.1-8.el7

## 163219 - Oracle Enterprise Linux ELSA-2016-2594 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0741, CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

### Description

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

ELSA-2016-2594

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006481.html>

OEL7

x86\_64

389-ds-base-1.3.5.10-11.el7

389-ds-base-libs-1.3.5.10-11.el7

389-ds-base-devel-1.3.5.10-11.el7

389-ds-base-snmp-1.3.5.10-11.el7

## 163221 - Oracle Enterprise Linux ELSA-2016-2615 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776, CVE-2016-8864

### Description

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

ELSA-2016-2615

## Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006494.html>

## OEL7

x86\_64  
bind-lite-devel-9.9.4-38.el7\_3  
bind-pkcs11-libs-9.9.4-38.el7\_3  
bind-sdb-9.9.4-38.el7\_3  
bind-pkcs11-utils-9.9.4-38.el7\_3  
bind-utils-9.9.4-38.el7\_3  
bind-chroot-9.9.4-38.el7\_3  
bind-devel-9.9.4-38.el7\_3  
bind-license-9.9.4-38.el7\_3  
bind-9.9.4-38.el7\_3  
bind-libs-9.9.4-38.el7\_3  
bind-pkcs11-devel-9.9.4-38.el7\_3  
bind-libs-lite-9.9.4-38.el7\_3  
bind-sdb-chroot-9.9.4-38.el7\_3  
bind-pkcs11-9.9.4-38.el7\_3

## 170739 - Amazon Linux AMI ALAS-2016-764 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6325, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797

## Description

The scan detected that the host is missing the following update:  
ALAS-2016-764

## Observation

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

<https://alas.aws.amazon.com/ALAS-2016-764.html>

## Amazon Linux AMI

noarch  
tomcat7-log4j-7.0.72-1.21.amzn1  
tomcat8-lib-8.0.38-1.65.amzn1  
tomcat7-el-2.2-api-7.0.72-1.21.amzn1  
tomcat6-javadoc-6.0.47-1.7.amzn1  
tomcat7-admin-webapps-7.0.72-1.21.amzn1  
tomcat7-lib-7.0.72-1.21.amzn1  
tomcat6-jsp-2.1-api-6.0.47-1.7.amzn1  
tomcat8-javadoc-8.0.38-1.65.amzn1  
tomcat7-servlet-3.0-api-7.0.72-1.21.amzn1  
tomcat6-servlet-2.5-api-6.0.47-1.7.amzn1  
tomcat7-webapps-7.0.72-1.21.amzn1  
tomcat8-log4j-8.0.38-1.65.amzn1  
tomcat8-webapps-8.0.38-1.65.amzn1  
tomcat6-el-2.1-api-6.0.47-1.7.amzn1  
tomcat6-docs-webapp-6.0.47-1.7.amzn1  
tomcat8-8.0.38-1.65.amzn1

tomcat8-docs-webapp-8.0.38-1.65.amzn1  
tomcat7-7.0.72-1.21.amzn1  
tomcat6-6.0.47-1.7.amzn1  
tomcat6-webapps-6.0.47-1.7.amzn1  
tomcat8-admin-webapps-8.0.38-1.65.amzn1  
tomcat6-lib-6.0.47-1.7.amzn1  
tomcat8-jsp-2.3-api-8.0.38-1.65.amzn1  
tomcat7-jsp-2.2-api-7.0.72-1.21.amzn1  
tomcat8-el-3.0-api-8.0.38-1.65.amzn1  
tomcat8-servlet-3.1-api-8.0.38-1.65.amzn1  
tomcat7-javadoc-7.0.72-1.21.amzn1  
tomcat7-docs-webapp-7.0.72-1.21.amzn1  
tomcat6-admin-webapps-6.0.47-1.7.amzn1

## 170740 - Amazon Linux AMI ALAS-2016-765 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

### Description

The scan detected that the host is missing the following update:  
ALAS-2016-765

### Observation

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

<https://alas.aws.amazon.com/ALAS-2016-765.html>

Amazon Linux AMI

x86\_64

policycoreutils-newrole-2.1.12-5.25.amzn1  
policycoreutils-2.1.12-5.25.amzn1  
policycoreutils-restorecond-2.1.12-5.25.amzn1  
policycoreutils-debuginfo-2.1.12-5.25.amzn1  
policycoreutils-python-2.1.12-5.25.amzn1

i686

policycoreutils-newrole-2.1.12-5.25.amzn1  
policycoreutils-debuginfo-2.1.12-5.25.amzn1  
policycoreutils-restorecond-2.1.12-5.25.amzn1  
policycoreutils-2.1.12-5.25.amzn1  
policycoreutils-python-2.1.12-5.25.amzn1

## 170741 - Amazon Linux AMI ALAS-2016-762 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7039, CVE-2016-8666

### Description

The scan detected that the host is missing the following update:  
ALAS-2016-762

### Observation

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

<https://alas.aws.amazon.com/ALAS-2016-762.html>

Amazon Linux AMI

i686

kernel-devel-4.4.30-32.54.amzn1

kernel-tools-4.4.30-32.54.amzn1

kernel-4.4.30-32.54.amzn1

kernel-headers-4.4.30-32.54.amzn1

kernel-tools-debuginfo-4.4.30-32.54.amzn1

perf-debuginfo-4.4.30-32.54.amzn1

kernel-debuginfo-common-i686-4.4.30-32.54.amzn1

kernel-tools-devel-4.4.30-32.54.amzn1

kernel-debuginfo-4.4.30-32.54.amzn1

perf-4.4.30-32.54.amzn1

noarch

kernel-doc-4.4.30-32.54.amzn1

x86\_64

kernel-devel-4.4.30-32.54.amzn1

kernel-tools-debuginfo-4.4.30-32.54.amzn1

perf-debuginfo-4.4.30-32.54.amzn1

kernel-4.4.30-32.54.amzn1

kernel-headers-4.4.30-32.54.amzn1

kernel-tools-4.4.30-32.54.amzn1

kernel-tools-devel-4.4.30-32.54.amzn1

perf-4.4.30-32.54.amzn1

kernel-debuginfo-4.4.30-32.54.amzn1

kernel-debuginfo-common-x86\_64-4.4.30-32.54.amzn1

### 170742 - Amazon Linux AMI ALAS-2016-763 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

#### Description

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

ALAS-2016-763

#### Observation

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

For more information see:

<https://alas.aws.amazon.com/ALAS-2016-763.html>

Amazon Linux AMI

noarch

cloud-init-0.7.6-2.13.amzn1

### 170743 - Amazon Linux AMI ALAS-2016-761 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

#### Description

The scan detected that the host is missing the following update:  
ALAS-2016-761

#### Observation

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

<https://alas.aws.amazon.com/ALAS-2016-761.html>

Amazon Linux AMI

x86\_64

memcached-debuginfo-1.4.15-9.13.amzn1

memcached-1.4.15-9.13.amzn1

memcached-devel-1.4.15-9.13.amzn1

i686

memcached-debuginfo-1.4.15-9.13.amzn1

memcached-1.4.15-9.13.amzn1

memcached-devel-1.4.15-9.13.amzn1

### **178235 - Gentoo Linux GLSA-201611-09 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-6258, CVE-2016-7092, CVE-2016-7093, CVE-2016-7094, CVE-2016-7777

#### Description

The scan detected that the host is missing the following update:  
GLSA-201611-09

#### Observation

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

<https://security.gentoo.org/glsa/201611-09>

Affected packages:

app-emulation/xen < 4.6.3-r3

app-emulation/xen-tools < 4.6.3-r2

### **178236 - Gentoo Linux GLSA-201611-05 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2014-8517

#### Description

The scan detected that the host is missing the following update:  
GLSA-201611-05

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201611-05>

Affected packages:

net-ftp/tntftp < 20141104

### 178237 - Gentoo Linux GLSA-201611-06 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-4342

#### Description

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

GLSA-201611-06

#### Observation

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

For more information see:

<https://security.gentoo.org/glsa/201611-06>

Affected packages:

sys-apps/xinetd < 2.3.15-r2

### 185477 - Ubuntu Linux 14.04 USN-3127-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9904, CVE-2015-3288, CVE-2016-3961, CVE-2016-7042

#### Description

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

USN-3127-1

#### 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-November/003624.html>

Ubuntu 14.04

linux-image-3.13.0-101-generic-lpae\_3.13.0-101.148  
linux-image-generic-lpae\_3.13.0.101.109  
linux-image-virtual\_3.13.0.101.109  
linux-image-3.13.0-101-powerpc64-smp\_3.13.0-101.148  
linux-image-3.13.0-101-powerpc-e500\_3.13.0-101.148  
linux-image-3.13.0-101-powerpc-smp\_3.13.0-101.148  
linux-image-powerpc-e500\_3.13.0.101.109  
linux-image-powerpc64-smp\_3.13.0.101.109  
linux-image-powerpc64-emb\_3.13.0.101.109  
linux-image-lowlatency\_3.13.0.101.109  
linux-image-powerpc-smp\_3.13.0.101.109  
linux-image-generic\_3.13.0.101.109



linux-image-powerpc-e500mc\_3.13.0.101.109  
linux-image-3.13.0-101-powerpc-e500mc\_3.13.0-101.148  
linux-image-3.13.0-101-lowlatency\_3.13.0-101.148  
linux-image-3.13.0-101-powerpc64-emb\_3.13.0-101.148  
linux-image-3.13.0-101-generic\_3.13.0-101.148

### 185482 - Ubuntu Linux 12.04 USN-3127-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9904, CVE-2015-3288, CVE-2016-3961, CVE-2016-7042

#### Description

The scan detected that the host is missing the following update:  
USN-3127-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003625.html>

Ubuntu 12.04

linux-image-generic-lts-trusty\_3.13.0.101.92  
linux-image-3.13.0-101-generic\_3.13.0-101.148~precise1  
linux-image-3.13.0-101-generic-lpae\_3.13.0-101.148~precise1  
linux-image-generic-lpae-lts-trusty\_3.13.0.101.92

### 191343 - Fedora Linux 24 FEDORA-2016-cd09eab674 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3796, CVE-2016-8859

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-cd09eab674

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

tre-0.8.0-18.20140228gitc2f5d13.fc24

### 191352 - Fedora Linux 23 FEDORA-2016-4094bd4ad6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-5388, CVE-2016-5425, CVE-2016-6325, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-4094bd4ad6

### 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/2016/11/?count=200&page=1>

Fedora Core 23

tomcat-8.0.38-1.fc23

## **191359 - Fedora Linux 23 FEDORA-2016-0ff6c3d84b Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2015-3796, CVE-2016-8859

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-0ff6c3d84b

### 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/2016/11/?count=200&page=1>

Fedora Core 23

tre-0.8.0-18.20140228gitc2f5d13.fc23

## **191362 - Fedora Linux 24 FEDORA-2016-c1b01b9278 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-5388, CVE-2016-5425, CVE-2016-6325, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-c1b01b9278

### 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/2016/11/?count=200&page=1>

Fedora Core 24

tomcat-8.0.38-1.fc24

## 20863 - IBM WebSphere Application Server Java SDK Multiple Vulnerabilities (October 2016 CPU)

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

Risk Level: Medium

CVE: CVE-2016-5573, CVE-2016-5597

### Description

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

### Observation

IBM WebSphere Application Server is a server engine for Java EE Web applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaws lie in the networking and in the virtual machine components. Successful exploitation could allow a remote attacker to affect confidentiality, integrity and availability.

## 20864 - IBM WebSphere Application Server Liberty Profile Java SDK Multiple Vulnerabilities (October 2016 CPU)

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

Risk Level: Medium

CVE: CVE-2016-5573, CVE-2016-5597

### Description

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

### Observation

IBM WebSphere Application Server Liberty Profile is a server engine for Java EE Web applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server Liberty Profile. The flaws lie in the networking and in the virtual machine components. Successful exploitation could allow a remote attacker to affect confidentiality, integrity and availability.

## 20867 - Cisco ASA Software DHCP Relay Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-6424

### Description

A denial of service vulnerability is present in some versions of Cisco ASA Software.

### Observation

Cisco ASA Software is the operating system used in Cisco firewall device.

A denial of service vulnerability is present in some versions of Cisco ASA Software. The flaw lies in DHCP Relay feature. Successful exploitation could allow an attacker to cause a denial of service condition.

## 130625 - Debian Linux 8.0 DSA-3711-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

### Description

The scan detected that the host is missing the following update:  
DSA-3711-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3711>

Debian 8.0

all

libmariadb-dev\_10.0.28-0+deb8u1  
mariadb-common\_10.0.28-0+deb8u1  
mariadb-server-10.0\_10.0.28-0+deb8u1  
mariadb-client\_10.0.28-0+deb8u1  
mariadb-connect-engine-10.0\_10.0.28-0+deb8u1  
mariadb-test\_10.0.28-0+deb8u1  
mariadb-oqgraph-engine-10.0\_10.0.28-0+deb8u1  
mariadb-client-10.0\_10.0.28-0+deb8u1  
mariadb-server-core-10.0\_10.0.28-0+deb8u1  
mariadb-server\_10.0.28-0+deb8u1  
mariadb-client-core-10.0\_10.0.28-0+deb8u1  
mariadb-test-10.0\_10.0.28-0+deb8u1

## 130628 - Debian Linux 8.0 DSA-3710-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9189, CVE-2016-9190

### Description

The scan detected that the host is missing the following update:  
DSA-3710-1

### Observation

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

<http://www.debian.org/security/2016/dsa-3710>

Debian 8.0

all

python3-pil.imagemagick\_2.6.1-2+deb8u3  
python-pil\_2.6.1-2+deb8u3  
python-pil-doc\_2.6.1-2+deb8u3  
python3-sane\_2.6.1-2+deb8u3  
python-imaging\_2.6.1-2+deb8u3  
python3-pil.imagemagick-dbg\_2.6.1-2+deb8u3  
python-imaging-tk\_2.6.1-2+deb8u3  
python3-pil\_2.6.1-2+deb8u3  
python-pil-dbg\_2.6.1-2+deb8u3  
python-pil.imagemagick-dbg\_2.6.1-2+deb8u3  
python-pil.imagemagick\_2.6.1-2+deb8u3

python3-pil-dbg\_2.6.1-2+deb8u3  
python3-sane-dbg\_2.6.1-2+deb8u3  
python-sane\_2.6.1-2+deb8u3  
python-sane-dbg\_2.6.1-2+deb8u3

## 163190 - Oracle Enterprise Linux ELSA-2016-2576 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

### Description

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

ELSA-2016-2576

### Observation

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

For more information see:

<http://oss.oracle.com/pipermail/el-errata/2016-November/006469.html>

OEL7

x86\_64

libguestfs-man-pages-ja-1.32.7-3.el7  
ocaml-libguestfs-devel-1.32.7-3.el7  
libguestfs-inspect-icons-1.32.7-3.el7  
libguestfs-bash-completion-1.32.7-3.el7  
ocaml-libguestfs-1.32.7-3.el7  
virt-v2v-1.32.7-3.el7  
libguestfs-man-pages-uk-1.32.7-3.el7  
libguestfs-gobject-1.32.7-3.el7  
libguestfs-devel-1.32.7-3.el7  
lua-guestfs-1.32.7-3.el7  
libguestfs-java-devel-1.32.7-3.el7  
ruby-libguestfs-1.32.7-3.el7  
python-libguestfs-1.32.7-3.el7  
libguestfs-tools-c-1.32.7-3.el7  
libguestfs-gobject-doc-1.32.7-3.el7  
libguestfs-rescue-1.32.7-3.el7  
libguestfs-tools-1.32.7-3.el7  
libguestfs-gobject-devel-1.32.7-3.el7  
perl-Sys-Guestfs-1.32.7-3.el7  
libguestfs-rsync-1.32.7-3.el7  
libguestfs-1.32.7-3.el7  
libguestfs-java-1.32.7-3.el7  
virt-dib-1.32.7-3.el7  
libguestfs-gfs2-1.32.7-3.el7  
libguestfs-javadoc-1.32.7-3.el7  
libguestfs-xfs-1.32.7-3.el7

## 163193 - Oracle Enterprise Linux ELSA-2016-2600 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572, CVE-2016-3948, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2600

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006487.html>

OEL7  
x86\_64  
squid-sysvinit-3.5.20-2.el7  
squid-migration-script-3.5.20-2.el7  
squid-3.5.20-2.el7

## **163202 - Oracle Enterprise Linux ELSA-2016-2573 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-5229, CVE-2015-7547, CVE-2016-3075

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2573

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006465.html>

OEL7  
x86\_64  
glibc-static-2.17-157.el7  
glibc-devel-2.17-157.el7  
glibc-utils-2.17-157.el7  
glibc-headers-2.17-157.el7  
glibc-2.17-157.el7  
nscd-2.17-157.el7  
glibc-common-2.17-157.el7

## **163207 - Oracle Enterprise Linux ELSA-2016-2589 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2013-1913, CVE-2013-1978, CVE-2016-4994

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2589

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006477.html>

OEL7

x86\_64

gimp-help-ca-2.8.2-1.el7

gimp-help-es-2.8.2-1.el7

gimp-help-ja-2.8.2-1.el7

gimp-help-fr-2.8.2-1.el7

gimp-help-ru-2.8.2-1.el7

gimp-help-en\_GB-2.8.2-1.el7

gimp-help-2.8.2-1.el7

gimp-help-de-2.8.2-1.el7

gimp-help-sl-2.8.2-1.el7

gimp-libs-2.8.16-3.el7

gimp-help-it-2.8.2-1.el7

gimp-help-ko-2.8.2-1.el7

gimp-help-nl-2.8.2-1.el7

gimp-help-da-2.8.2-1.el7

gimp-help-nn-2.8.2-1.el7

gimp-2.8.16-3.el7

gimp-help-zh\_CN-2.8.2-1.el7

gimp-devel-tools-2.8.16-3.el7

gimp-help-pt\_BR-2.8.2-1.el7

gimp-devel-2.8.16-3.el7

gimp-help-el-2.8.2-1.el7

gimp-help-sv-2.8.2-1.el7

### 20852 - (HT207274) Apple iTunes Multiple Vulnerabilities Prior To 12.5.2

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

Risk Level: Medium

CVE: CVE-2016-4613, CVE-2016-7578

#### 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 the WebKit component. Successful exploitation could allow an attacker to execute arbitrary code or disclose sensitive information.

### 20862 - (SOL35322517) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-8864

#### Description

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

### 20872 - (APSB16-35) Vulnerability In Adobe Connect

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

Risk Level: Medium

CVE: CVE-2016-7851

#### Description

A vulnerability is present in some versions of Adobe Connect.

#### Observation

Adobe Connect is a network meeting solution.

A vulnerability is present in some versions of Adobe Connect. The flaw lies in the events registration module. Successful exploitation could allow an attacker to launch cross-site scripting attacks.

The update provided by Adobe bulletin APSB16-35 resolves this issue. The target system appears to be missing this update.

### 20874 - (SOL05046514) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7979

#### Description

A denial of service 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 denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in NTP network if it is configured for broadcast operations. Successful exploitation could allow an attacker to cause a denial of service condition.

### 141360 - Red Hat Enterprise Linux RHSA-2016-2765 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

#### Description

The scan detected that the host is missing the following update:  
RHSA-2016-2765

#### Observation

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

<https://rhn.redhat.com/errata/RHSA-2016-2765.html>

RHEL6S  
x86\_64



389-ds-base-devel-1.2.11.15-84.el6\_8  
389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

i386

389-ds-base-devel-1.2.11.15-84.el6\_8  
389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

RHEL6WS

x86\_64  
389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

i386

389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

RHEL6D

x86\_64  
389-ds-base-devel-1.2.11.15-84.el6\_8  
389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

i386

389-ds-base-devel-1.2.11.15-84.el6\_8  
389-ds-base-debuginfo-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

## 160166 - CentOS 6 CESA-2016-2674 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6313

### Description

The scan detected that the host is missing the following update:  
CESA-2016-2674

### Observation

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

<http://lists.centos.org/pipermail/centos-announce/2016-November/022141.html>

CentOS 6

x86\_64  
libcrypt-devel-1.4.5-12.el6\_8  
libcrypt-1.4.5-12.el6\_8

i686

libcrypt-devel-1.4.5-12.el6\_8

## 163188 - Oracle Enterprise Linux ELSA-2016-2606 Update Is Not Installed

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

Risk Level: Medium

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

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2606

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006491.html>

OEL7  
x86\_64  
postgresql-plpython-9.2.18-1.el7  
postgresql-server-9.2.18-1.el7  
postgresql-devel-9.2.18-1.el7  
postgresql-9.2.18-1.el7  
postgresql-contrib-9.2.18-1.el7  
postgresql-pltcl-9.2.18-1.el7  
postgresql-docs-9.2.18-1.el7  
postgresql-upgrade-9.2.18-1.el7  
postgresql-test-9.2.18-1.el7  
postgresql-libs-9.2.18-1.el7  
postgresql-plperl-9.2.18-1.el7

## 163189 - Oracle Enterprise Linux ELSA-2016-2765 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4992, CVE-2016-5405, CVE-2016-5416

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2765

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006511.html>

OEL6  
x86\_64  
389-ds-base-devel-1.2.11.15-84.el6\_8  
389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

i386  
389-ds-base-devel-1.2.11.15-84.el6\_8

389-ds-base-1.2.11.15-84.el6\_8  
389-ds-base-libs-1.2.11.15-84.el6\_8

### 163194 - Oracle Enterprise Linux ELSA-2016-2603 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5361

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2603

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006493.html>

OEL7  
x86\_64  
libreswan-3.15-8.0.1.el7

### 163197 - Oracle Enterprise Linux ELSA-2016-2575 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux 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:  
ELSA-2016-2575

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006466.html>

OEL7  
x86\_64  
libcurl-devel-7.29.0-35.el7  
curl-7.29.0-35.el7  
libcurl-7.29.0-35.el7

### 163204 - Oracle Enterprise Linux ELSA-2016-2583 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-5211, CVE-2015-5194, CVE-2015-5195, CVE-2015-5196, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7974, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8158, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-2518

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2583

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006472.html>

OEL7  
x86\_64  
ntp-doc-4.2.6p5-25.0.1.el7  
ntp-perl-4.2.6p5-25.0.1.el7  
ntp-4.2.6p5-25.0.1.el7  
snmp-4.2.6p5-25.0.1.el7  
ntpdate-4.2.6p5-25.0.1.el7

### **163216 - Oracle Enterprise Linux ELSA-2016-2597 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-5410

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2597

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006488.html>

OEL7  
x86\_64  
python-firewall-0.4.3.2-8.el7  
firewall-applet-0.4.3.2-8.el7  
firewalld-filesystem-0.4.3.2-8.el7  
firewalld-0.4.3.2-8.el7  
firewall-config-0.4.3.2-8.el7

### **170738 - Amazon Linux AMI ALAS-2016-766 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624

#### Description

The scan detected that the host is missing the following update:  
ALAS-2016-766

#### Observation

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

<https://alas.aws.amazon.com/ALAS-2016-766.html>

Amazon Linux AMI

x86\_64

libcurl-7.47.1-9.66.amzn1

curl-7.47.1-9.66.amzn1

libcurl-devel-7.47.1-9.66.amzn1

curl-debuginfo-7.47.1-9.66.amzn1

i686

libcurl-7.47.1-9.66.amzn1

curl-7.47.1-9.66.amzn1

libcurl-devel-7.47.1-9.66.amzn1

curl-debuginfo-7.47.1-9.66.amzn1

### 191350 - Fedora Linux 24 FEDORA-2016-e38196b52a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

#### Description

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

FEDORA-2016-e38196b52a

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

bind-9.10.4-2.P4.fc24

### 20861 - (VMSA-2016-0017) VMware Fusion Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-5329

#### Description

An information disclosure vulnerability is present in some versions of VMware Fusion.

#### Observation

VMware Fusion is a popular virtualization platform.

An information disclosure vulnerability is present in some versions of VMware Fusion. The flaw lies in an unspecified component of this software. Successful exploitation could allow an attacker to retrieve sensitive data bypassing the kASLR protection mechanism.

### 20873 - (SOL06288381) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7977, CVE-2015-7978

#### Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in the ntpd process. Successful exploitation could allow an attacker to cause ntpd to dereference a NULL pointer or exhaust its call stack, in both cases leading to a crash of the ntpd service.

### **163191 - Oracle Enterprise Linux ELSA-2016-2591 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-3119, CVE-2016-3120

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2591

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006479.html>

OEL7

x86\_64

libkadm5-1.14.1-26.el7

krb5-devel-1.14.1-26.el7

krb5-server-1.14.1-26.el7

krb5-server-ldap-1.14.1-26.el7

krb5-pkinit-1.14.1-26.el7

krb5-workstation-1.14.1-26.el7

krb5-libs-1.14.1-26.el7

### **163192 - Oracle Enterprise Linux ELSA-2016-2610 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-7795

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2610

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006496.html>

OEL7

x86\_64  
systemd-journal-gateway-219-30.0.1.el7\_3.3  
libgudev1-219-30.0.1.el7\_3.3  
systemd-python-219-30.0.1.el7\_3.3  
systemd-libs-219-30.0.1.el7\_3.3  
systemd-networkd-219-30.0.1.el7\_3.3  
systemd-devel-219-30.0.1.el7\_3.3  
libgudev1-devel-219-30.0.1.el7\_3.3  
systemd-sysv-219-30.0.1.el7\_3.3  
systemd-resolved-219-30.0.1.el7\_3.3  
systemd-219-30.0.1.el7\_3.3

### 163210 - Oracle Enterprise Linux ELSA-2016-2601 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5384

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2601

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006489.html>

OEL7  
x86\_64  
fontconfig-2.10.95-10.el7  
fontconfig-devel-2.10.95-10.el7  
fontconfig-devel-doc-2.10.95-10.el7

### 163215 - Oracle Enterprise Linux ELSA-2016-2577 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5160, CVE-2015-5313, CVE-2016-5008

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2577

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006468.html>

OEL7  
x86\_64  
libvirt-daemon-driver-lxc-2.0.0-10.el7  
libvirt-daemon-kvm-2.0.0-10.el7  
libvirt-lock-sanlock-2.0.0-10.el7  
libvirt-devel-2.0.0-10.el7

libvirt-daemon-2.0.0-10.el7  
libvirt-daemon-driver-nwfilter-2.0.0-10.el7  
libvirt-daemon-lxc-2.0.0-10.el7  
libvirt-daemon-driver-secret-2.0.0-10.el7  
libvirt-daemon-driver-interface-2.0.0-10.el7  
libvirt-daemon-driver-storage-2.0.0-10.el7  
libvirt-daemon-driver-nodedev-2.0.0-10.el7  
libvirt-client-2.0.0-10.el7  
libvirt-2.0.0-10.el7  
libvirt-daemon-config-nwfilter-2.0.0-10.el7  
libvirt-docs-2.0.0-10.el7  
libvirt-nss-2.0.0-10.el7  
libvirt-daemon-driver-network-2.0.0-10.el7  
libvirt-login-shell-2.0.0-10.el7  
libvirt-daemon-driver-qemu-2.0.0-10.el7  
libvirt-daemon-config-network-2.0.0-10.el7

### 178238 - Gentoo Linux GLSA-201611-07 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3255

#### Description

The scan detected that the host is missing the following update:  
GLSA-201611-07

#### Observation

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

<https://security.gentoo.org/glsa/201611-07>

Affected packages:

sys-auth/polkit < 0.113

### 182168 - FreeBSD gitlab Directory Traversal Via "import/export" Feature (10968dfd-a687-11e6-b2d3-60a44ce6887b)

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

Risk Level: Medium

CVE: CVE-2016-9086

#### Description

The scan detected that the host is missing the following update:  
gitlab -- Directory traversal via "import/export" feature (10968dfd-a687-11e6-b2d3-60a44ce6887b)

#### Observation

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

<http://www.vuxml.org/freebsd/10968dfd-a687-11e6-b2d3-60a44ce6887b.html>

Affected packages:

8.10.0 <= rubygem-gitlab <= 8.10.12

8.11.0 <= rubygem-gitlab <= 8.11.9

8.12.0 <= rubygem-gitlab <= 8.12.7



8.13.0 <= rubygem-gitlab <= 8.13.2

### 185474 - Ubuntu Linux 16.04 USN-3128-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7042

#### Description

The scan detected that the host is missing the following update:  
USN-3128-1

#### 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-November/003626.html>

Ubuntu 16.04

linux-image-powerpc64-smp\_4.4.0.47.50  
linux-image-generic-lpae\_4.4.0.47.50  
linux-image-4.4.0-47-powerpc64-smp\_4.4.0-47.68  
linux-image-virtual\_4.4.0.47.50  
linux-image-generic\_4.4.0.47.50  
linux-image-powerpc-e500mc\_4.4.0.47.50  
linux-image-4.4.0-47-powerpc-e500mc\_4.4.0-47.68  
linux-image-lowlatency\_4.4.0.47.50  
linux-image-4.4.0-47-powerpc64-emb\_4.4.0-47.68  
linux-image-powerpc-smp\_4.4.0.47.50  
linux-image-4.4.0-47-powerpc-smp\_4.4.0-47.68  
linux-image-4.4.0-47-generic\_4.4.0-47.68  
linux-image-4.4.0-47-generic-lpae\_4.4.0-47.68  
linux-image-powerpc64-emb\_4.4.0.47.50  
linux-image-4.4.0-47-lowlatency\_4.4.0-47.68

### 185475 - Ubuntu Linux 16.10 USN-3129-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7042

#### Description

The scan detected that the host is missing the following update:  
USN-3129-2

#### Observation

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

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003630.html>

Ubuntu 16.10

linux-image-raspi2\_4.8.0.1018.21  
linux-image-4.8.0-1018-raspi2\_4.8.0-1018.21

## 185476 - Ubuntu Linux 14.04 USN-3128-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7042

### Description

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

USN-3128-2

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003627.html>

Ubuntu 14.04

linux-image-4.4.0-47-generic-lpae\_4.4.0-47.68~14.04.1  
linux-image-powerpc-e500mc-lts-xenial\_4.4.0.47.34  
linux-image-4.4.0-47-powerpc64-emb\_4.4.0-47.68~14.04.1  
linux-image-4.4.0-47-powerpc64-smp\_4.4.0-47.68~14.04.1  
linux-image-lowlatency-lts-xenial\_4.4.0.47.34  
linux-image-4.4.0-47-powerpc-smp\_4.4.0-47.68~14.04.1  
linux-image-powerpc64-emb-lts-xenial\_4.4.0.47.34  
linux-image-4.4.0-47-generic\_4.4.0-47.68~14.04.1  
linux-image-generic-lpae-lts-xenial\_4.4.0.47.34  
linux-image-generic-lts-xenial\_4.4.0.47.34  
linux-image-4.4.0-47-powerpc-e500mc\_4.4.0-47.68~14.04.1  
linux-image-4.4.0-47-lowlatency\_4.4.0-47.68~14.04.1  
linux-image-powerpc-smp-lts-xenial\_4.4.0.47.34  
linux-image-powerpc64-smp-lts-xenial\_4.4.0.47.34

## 185480 - Ubuntu Linux 16.04 USN-3128-3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7042

### Description

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

USN-3128-3

### Observation

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

For more information see:

<https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003628.html>

Ubuntu 16.04

linux-image-snapdragon\_4.4.0.1035.27  
linux-image-4.4.0-1035-snapdragon\_4.4.0-1035.39

## 185483 - Ubuntu Linux 16.10 USN-3129-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7042

### Description

The scan detected that the host is missing the following update:  
USN-3129-1

### 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-November/003629.html>

Ubuntu 16.10

linux-image-4.8.0-27-generic-lpae\_4.8.0-27.29  
linux-image-lowlatency\_4.8.0.27.36  
linux-image-powerpc-e500mc\_4.8.0.27.36  
linux-image-powerpc-smp\_4.8.0.27.36  
linux-image-powerpc64-emb\_4.8.0.27.36  
linux-image-virtual\_4.8.0.27.36  
linux-image-4.8.0-27-lowlatency\_4.8.0-27.29  
linux-image-4.8.0-27-powerpc-e500mc\_4.8.0-27.29  
linux-image-4.8.0-27-powerpc64-emb\_4.8.0-27.29  
linux-image-4.8.0-27-powerpc-smp\_4.8.0-27.29  
linux-image-4.8.0-27-generic\_4.8.0-27.29  
linux-image-generic\_4.8.0.27.36  
linux-image-powerpc64-smp\_4.8.0.27.36  
linux-image-generic-lpae\_4.8.0.27.36

## 191345 - Fedora Linux 23 FEDORA-2016-6c789ba91d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2089, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8880, CVE-2016-8881, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-6c789ba91d

### 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/2016/11/?count=200&page=1>

Fedora Core 23

jasper-1.900.13-1.fc23

## 191351 - Fedora Linux 24 FEDORA-2016-e0f0d48142 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2089, CVE-2016-8690, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8880, CVE-2016-8881, CVE-2016-8882, CVE-2016-8883, CVE-2016-8884, CVE-2016-8885, CVE-2016-8886, CVE-2016-8887

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-e0f0d48142

#### 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/2016/11/?count=200&page=2>

Fedora Core 24

jasper-1.900.13-1.fc24

### **130626 - Debian Linux 8.0 DSA-3712-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2015-8971

#### Description

The scan detected that the host is missing the following update:  
DSA-3712-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3712>

Debian 8.0

all

terminology\_0.7.0-1+deb8u1

### **130627 - Debian Linux 8.0 DSA-3713-1 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

The scan detected that the host is missing the following update:  
DSA-3713-1

#### Observation

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

<http://www.debian.org/security/2016/dsa-3713>

Debian 8.0  
all  
libgstreamer-plugins-bad0.10-dev\_0.10.23-7.4+deb8u1  
libgstreamer-plugins-bad0.10-0\_0.10.23-7.4+deb8u1  
gstreamer0.10-plugins-bad\_0.10.23-7.4+deb8u1  
gstreamer0.10-plugins-bad-dbg\_0.10.23-7.4+deb8u1

### 163198 - Oracle Enterprise Linux ELSA-2016-2581 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-0764

#### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2581

#### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006473.html>

OEL7

x86\_64

NetworkManager-libnm-1.4.0-12.el7

libnm-gtk-devel-1.4.0-2.el7

network-manager-applet-1.4.0-2.el7

NetworkManager-tui-1.4.0-12.el7

libnma-devel-1.4.0-2.el7

libnl3-cli-3.2.28-2.el7

NetworkManager-libnm-devel-1.4.0-12.el7

libnl3-devel-3.2.28-2.el7

NetworkManager-bluetooth-1.4.0-12.el7

libnma-1.4.0-2.el7

NetworkManager-glib-1.4.0-12.el7

NetworkManager-adsl-1.4.0-12.el7

NetworkManager-config-server-1.4.0-12.el7

NetworkManager-1.4.0-12.el7

NetworkManager-dispatcher-routing-rules-1.4.0-12.el7

NetworkManager-team-1.4.0-12.el7

NetworkManager-wwan-1.4.0-12.el7

NetworkManager-libreswan-gnome-1.2.4-1.el7

libnl3-doc-3.2.28-2.el7

libnm-gtk-1.4.0-2.el7

NetworkManager-glib-devel-1.4.0-12.el7

libnl3-3.2.28-2.el7

NetworkManager-libreswan-1.2.4-1.el7

nm-connection-editor-1.4.0-2.el7

NetworkManager-wifi-1.4.0-12.el7

### 163203 - Oracle Enterprise Linux ELSA-2016-2593 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7091

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2593

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006484.html>

OEL7  
x86\_64  
sudo-1.8.6p7-20.el7  
sudo-devel-1.8.6p7-20.el7

## **163220 - Oracle Enterprise Linux ELSA-2016-2602 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-3099

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2602

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006490.html>

OEL7  
x86\_64  
mod\_nss-1.0.14-7.el7

## **163222 - Oracle Enterprise Linux ELSA-2016-2605 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-5011

### Description

The scan detected that the host is missing the following update:  
ELSA-2016-2605

### Observation

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

<http://oss.oracle.com/pipermail/el-errata/2016-November/006492.html>

OEL7  
x86\_64  
libmount-devel-2.23.2-33.0.1.el7

uidd-2.23.2-33.0.1.el7  
util-linux-2.23.2-33.0.1.el7  
libuuid-devel-2.23.2-33.0.1.el7  
libmount-2.23.2-33.0.1.el7  
libblkid-2.23.2-33.0.1.el7  
libblkid-devel-2.23.2-33.0.1.el7  
libuuid-2.23.2-33.0.1.el7

### 182167 - FreeBSD lives Insecure Files Permissions (a8e9d834-a916-11e6-b9b4-bcaec524bf84)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Description

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

lives -- insecure files permissions (a8e9d834-a916-11e6-b9b4-bcaec524bf84)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/a8e9d834-a916-11e6-b9b4-bcaec524bf84.html>

Affected packages:

lives < 2.8.1

### 182169 - FreeBSD chromium Multiple Vulnerabilities (a3473f5a-a739-11e6-afaa-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2016-5199, CVE-2016-5200, CVE-2016-5201, CVE-2016-5202

#### Description

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

chromium -- multiple vulnerabilities (a3473f5a-a739-11e6-afaa-e8e0b747a45a)

#### Observation

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

For more information see:

<http://www.vuxml.org/freebsd/a3473f5a-a739-11e6-afaa-e8e0b747a45a.html>

Affected packages:

chromium < 54.0.2840.100

chromium-npapi < 54.0.2840.100

chromium-pulse < 54.0.2840.100

### 182170 - FreeBSD mozilla Multiple Vulnerabilities (d1853110-07f4-4645-895b-6fd462ad0589)

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

Risk Level: Low

CVE: CVE-2016-5289, CVE-2016-5290, CVE-2016-5291, CVE-2016-5292, CVE-2016-5293, CVE-2016-5294, CVE-2016-5295, CVE-2016-5296, CVE-2016-5297, CVE-2016-5298, CVE-2016-5299, CVE-2016-9061, CVE-2016-9062, CVE-2016-9063, CVE-2016-9064, CVE-2016-9065, CVE-2016-9066, CVE-2016-9067, CVE-2016-9068, CVE-2016-9070, CVE-2016-9071, CVE-2016-9072, CVE-2016-

9073, CVE-2016-9074, CVE-2016-9075, CVE-2016-9076, CVE-2016-9077

#### Description

The scan detected that the host is missing the following update:  
mozilla -- multiple vulnerabilities (d1853110-07f4-4645-895b-6fd462ad0589)

#### Observation

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

<http://www.vuxml.org/freebsd/d1853110-07f4-4645-895b-6fd462ad0589.html>

Affected packages:

firefox < 50.0\_1,1  
seamonkey < 2.47  
linux-seamonkey < 2.47  
firefox-esr < 45.5.0,1  
linux-firefox < 45.5.0,2  
libxul < 45.5.0  
thunderbird < 45.5.0  
linux-thunderbird < 45.5.0

### **182172 - FreeBSD openssl Multiple Vulnerabilities (50751310-a763-11e6-a881-b499baebfeaf)**

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

Risk Level: Low

CVE: CVE-2016-7053, CVE-2016-7054, CVE-2016-7055

#### Description

The scan detected that the host is missing the following update:  
openssl -- multiple vulnerabilities (50751310-a763-11e6-a881-b499baebfeaf)

#### Observation

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

<http://www.vuxml.org/freebsd/50751310-a763-11e6-a881-b499baebfeaf.html>

Affected packages:

openssl-devel < 1.1.0c

### **191346 - Fedora Linux 24 FEDORA-2016-3eb5a55123 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9013, CVE-2016-9014

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-3eb5a55123

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

python-django-1.9.11-1.fc24

### 191347 - Fedora Linux 24 FEDORA-2016-112b333bdf Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7076

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-112b333bdf

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

sudo-1.8.18p1-1.fc24

### 191348 - Fedora Linux 24 FEDORA-2016-66c70cadb4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-66c70cadb4

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

memcached-1.4.25-2.fc24

### 191349 - Fedora Linux 23 FEDORA-2016-f7a079f775 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7966, CVE-2016-7967, CVE-2016-7968

#### Description

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

FEDORA-2016-f7a079f775

#### 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/2016/11/?count=200&page=1>

Fedora Core 23

kdepimlibs-4.14.10-15.fc23

### **191354 - Fedora Linux 25 FEDORA-2016-c1cbcc4528 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7035

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-c1cbcc4528

#### 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/2016/11/?count=200&page=1>

Fedora Core 25

pacemaker-1.1.15-3.fc25

### **191355 - Fedora Linux 23 FEDORA-2016-4df986a71f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-4df986a71f

#### 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/2016/11/?count=200&page=1>

Fedora Core 23

memcached-1.4.17-5.fc23

### **191356 - Fedora Linux 24 FEDORA-2016-00d2f5c19f Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-9085

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-00d2f5c19f

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

mingw-libwebp-0.5.1-2.fc24

### **191357 - Fedora Linux 23 FEDORA-2016-21f0de504c Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-7945, CVE-2016-7946

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-21f0de504c

#### 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/2016/11/?count=200&page=1>

Fedora Core 23

libXi-1.7.8-2.fc23

### **191358 - Fedora Linux 24 FEDORA-2016-2b27b075ee 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-2016-2b27b075ee

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

libgit2-0.24.3-1.fc24

### 191360 - Fedora Linux 24 FEDORA-2016-94d1c64fe2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8637

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-94d1c64fe2

#### 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/2016/11/?count=200&page=1>

Fedora Core 24

dracut-044-21.fc24

### 191361 - Fedora Linux 24 FEDORA-2016-c671aae490 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194, CVE-2016-5198

#### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-c671aae490

#### 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/2016/11/?count=200&page=2>

Fedora Core 24

chromium-54.0.2840.90-3.fc24

chromium-native\_client-54.0.2840.59-1.20161013git090f907.fc24

### 20878 - (SOL13304944) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2015-7974

#### Description

A 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 vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in NTP network when multiple NTP servers are configured using symmetric key authentication. Successful exploitation could allow an attacker to spoofing attack.

### **191344 - Fedora Linux 23 FEDORA-2016-da6b1d277b Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8576, CVE-2016-8578, CVE-2016-8669, CVE-2016-8910, CVE-2016-9102, CVE-2016-9103, CVE-2016-9104, CVE-2016-9105, CVE-2016-9106

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-da6b1d277b

### 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/2016/11/?count=200&page=1>

Fedora Core 23

xen-4.5.5-3.fc23

### **191353 - Fedora Linux 24 FEDORA-2016-0d1a8ee35b Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-2016-8576, CVE-2016-8578, CVE-2016-8669, CVE-2016-8910, CVE-2016-9102, CVE-2016-9103, CVE-2016-9104, CVE-2016-9105, CVE-2016-9106

### Description

The scan detected that the host is missing the following update:  
FEDORA-2016-0d1a8ee35b

### 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/2016/11/?count=200&page=2>

Fedora Core 24

xen-4.6.3-7.fc24

## **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.

### **32944 - Oracle Solaris 137322-04 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2008-6536

Update Details

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

**32951 - Oracle Solaris 137321-04 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2008-6536

Update Details

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

**20765 - (MS16-132) Security Update for Microsoft Graphics Component (3199120)**

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

Risk Level: High

CVE: CVE-2016-7205, CVE-2016-7210, CVE-2016-7217

Update Details

Risk is updated

**20795 - (MS16-134) Security Update for Common Log File System Driver (3193706)**

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

Risk Level: High

CVE: CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, CVE-2016-7184

Update Details

Risk is updated

**20798 - (MS16-133) Security Update for Microsoft Office (3199168)**

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

Risk Level: High

CVE: CVE-2016-7213, CVE-2016-7228, CVE-2016-7229, CVE-2016-7230, CVE-2016-7231, CVE-2016-7232, CVE-2016-7233, CVE-2016-7234, CVE-2016-7235, CVE-2016-7236, CVE-2016-7244, CVE-2016-7245

Update Details

Risk is updated

**163185 - Oracle Enterprise Linux ELSA-2016-2658 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Update Details

FASLScript is updated

**20757 - (MS16-135) Security Update for Windows Kernel-Mode Drivers (3199135)**

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

Risk Level: High

CVE: CVE-2016-7214, CVE-2016-7215, CVE-2016-7218, CVE-2016-7246, CVE-2016-7255

Update Details

Risk is updated

**32160 - Oracle Solaris 136882-05 Update Is Not Installed**

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

Risk Level: High

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

Update Details

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

**32163 - Oracle Solaris 136883-05 Update Is Not Installed**

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

Risk Level: High

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

Update Details

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

**33116 - Oracle Solaris 150383-17 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

**88819 - Slackware Linux 14.0, 14.1, 14.2 SSA:2016-305-01 Update Is Not Installed**

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

Risk Level: High

CVE: CVE-2016-5195

Update Details

Risk is updated

#### 170734 - Amazon Linux AMI ALAS-2016-757 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

#### 185447 - Ubuntu Linux 16.04 USN-3106-4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

#### 185448 - Ubuntu Linux 14.04 USN-3106-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

#### 185449 - Ubuntu Linux 12.04 USN-3104-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

#### 185450 - Ubuntu Linux 12.04 USN-3104-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

#### 185451 - Ubuntu Linux 16.04 USN-3106-3 Update Is Not Installed

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



Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

**185452 - Ubuntu Linux 16.10 USN-3107-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

**185453 - Ubuntu Linux 14.04 USN-3105-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

**185454 - Ubuntu Linux 16.04 USN-3106-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

**185455 - Ubuntu Linux 12.04 USN-3105-2 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

**185462 - Ubuntu Linux 16.10 USN-3107-2 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes  
Risk Level: High  
CVE: CVE-2016-5195

[Update Details](#)

Risk is updated

---

### 191298 - Fedora Linux 23 FEDORA-2016-c3558808cd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

#### Update Details

Risk is updated

### 191300 - Fedora Linux 24 FEDORA-2016-db4b75b352 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

#### Update Details

Risk is updated

### 191308 - Fedora Linux 25 FEDORA-2016-c8a0c7eece Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5195

#### Update Details

Risk is updated

### 20609 - Cisco IOS Application-Hosting Framework Unauthorized File Access Vulnerability

Category: SSH Module -> NonIntrusive -> Cisco IOS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6410

#### Update Details

Recommendation is updated

### 31558 - Oracle Solaris 119783-38 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 119784-38 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

**14558 - Microsoft TURKTRUST.Inc Fraudulent Certificates Spoofing (2798897)**

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated FASLScript is updated

**37533 - IBM AIX IV84984 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-1285, CVE-2016-1286

Update Details

FASLScript is updated

**163186 - Oracle Enterprise Linux ELSA-2016-2674 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2016-6313

Update Details

FASLScript is updated

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

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0739

Update Details

Recommendation is updated

**37544 - IBM AIX IV86116 Update Is Not Installed**

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

Risk Level: Medium

CVE: CVE-2015-7575, CVE-2016-0266

Update Details

FASLScript is updated

### 20758 - (MS16-138) Security Update to Microsoft Virtual Hard Drive (3199647)

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

Risk Level: Low

CVE: CVE-2016-7223, CVE-2016-7224, CVE-2016-7225, CVE-2016-7226

#### Update Details

Risk is updated

### 33319 - Oracle Solaris 151913-08 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 33323 - Oracle Solaris 151912-08 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

#### Update Details

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

### 182098 - FreeBSD gnupg Attacker Who Obtains 4640 Bits From The RNG Can Trivially Predict The Next 160 Bits Of Output (e1c71d8d-64d9-11e6-

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

Risk Level: Low

CVE: CVE-2016-6313

#### 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

## DELETED CHECKS

### 11530 - (MS11-016) Microsoft Microsoft Groove Insecure Library Loading RCE (2494047)

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

Risk Level: High

CVE: CVE-2010-3146

## ADDITIONAL NOTES

- **11530** - is replaced by FID 20865.

## HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

## MCAFFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2016 McAfee, Inc.  
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates