2016-JUN-16
FSL version 7.5.828

# MCAFEE FOUNDSTONE FSL UPDATE

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

## NEW CHECKS

### 20206 - (APSB16-18) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-4125, CVE-2016-4127, CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE-2016-4133, CVE-2016-4134, CVE-2016-4135, CVE-2016-4136, CVE-2016-4137, CVE-2016-4138, CVE-2016-4139, CVE-2016-4140, CVE-2016-4141, CVE-2016-4142, CVE-2016-4143, CVE-2016-4144, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-4148, CVE-2016-4149, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153, CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic or memory issues. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-18 resolves the issues. The target system is missing this update.

### 20207 - (APSB16-18) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4122, CVE-2016-4123, CVE-2016-4124, CVE-2016-4125, CVE-2016-4127, CVE-2016-4128, CVE-2016-4129, CVE-2016-4130, CVE-2016-4131, CVE-2016-4132, CVE-2016-4133, CVE-2016-4134, CVE-2016-4135, CVE-2016-4136, CVE-2016-4137, CVE-2016-4138, CVE-2016-4139, CVE-2016-4140, CVE-2016-4141, CVE-2016-4142, CVE-2016-4143, CVE-2016-4144, CVE-2016-4145, CVE-2016-4146, CVE-2016-4147, CVE-2016-4148, CVE-2016-4149, CVE-2016-4150, CVE-2016-4151, CVE-2016-4152, CVE-2016-4153, CVE-2016-4154, CVE-2016-4155, CVE-2016-4156, CVE-2016-4166, CVE-2016-4171

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic or memory issues. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-18 resolves the issues. The target system is missing this update.

## 130516 - Debian Linux 8.0 DSA-3601-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2806

Description

The scan detected that the host is missing the following update:
DSA-3601-1

Observation

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

http://www.debian.org/security/2016/dsa-3601

Debian 8.0
all
icedove_1:45.1.0-1~deb8u1

## 144663 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1559-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5260, CVE-2015-5261, CVE-2016-0749, CVE-2016-2150

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1559-1

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-June/002108.html

SuSE SLES 12 SP1
x86_64
spice-debugsource-0.12.5-4.1
libspice-server1-debuginfo-0.12.5-4.1
libspice-server1-0.12.5-4.1

SuSE SLED 12 SP1
x86_64
spice-debugsource-0.12.5-4.1
libspice-server1-debuginfo-0.12.5-4.1
libspice-server1-0.12.5-4.1

## 144665 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1570-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1570-1

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-June/002114.html

SuSE SLES 12
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1

SuSE SLES 12 SP1
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1

SuSE SLED 12
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
libMagick++-6_Q16-3-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
ImageMagick-6.8.8.1-25.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-25.1

SuSE SLED 12 SP1
x86_64
libMagickWand-6_Q16-1-debuginfo-6.8.8.1-25.1
ImageMagick-debugsource-6.8.8.1-25.1
libMagick++-6_Q16-3-6.8.8.1-25.1
ImageMagick-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-6.8.8.1-25.1
libMagickCore-6_Q16-1-32bit-6.8.8.1-25.1
libMagickCore-6_Q16-1-debuginfo-32bit-6.8.8.1-25.1
libMagickWand-6_Q16-1-6.8.8.1-25.1
ImageMagick-6.8.8.1-25.1
libMagick++-6_Q16-3-debuginfo-6.8.8.1-25.1

## 144666 - SuSE Linux 13.2 openSUSE-SU-2016:1534-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1534-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00031.html

SuSE Linux 13.2
i586
ImageMagick-extra-6.8.9.8-21.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-21.1
ImageMagick-debugsource-6.8.9.8-21.1
perl-PerlMagick-debuginfo-6.8.9.8-21.1
perl-PerlMagick-6.8.9.8-21.1
ImageMagick-6.8.9.8-21.1
ImageMagick-debuginfo-6.8.9.8-21.1
ImageMagick-extra-debuginfo-6.8.9.8-21.1
libMagickWand-6_Q16-2-6.8.9.8-21.1
libMagick++-devel-6.8.9.8-21.1
ImageMagick-devel-6.8.9.8-21.1
libMagickCore-6_Q16-2-6.8.9.8-21.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-21.1
libMagick++-6_Q16-5-6.8.9.8-21.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-21.1

noarch
ImageMagick-doc-6.8.9.8-21.1

x86_64
ImageMagick-devel-32bit-6.8.9.8-21.1
libMagick++-6_Q16-5-debuginfo-32bit-6.8.9.8-21.1
libMagickCore-6_Q16-2-32bit-6.8.9.8-21.1
ImageMagick-extra-6.8.9.8-21.1
libMagickWand-6_Q16-2-debuginfo-6.8.9.8-21.1
ImageMagick-debugsource-6.8.9.8-21.1
perl-PerlMagick-debuginfo-6.8.9.8-21.1
libMagickWand-6_Q16-2-32bit-6.8.9.8-21.1
perl-PerlMagick-6.8.9.8-21.1
ImageMagick-6.8.9.8-21.1
libMagickCore-6_Q16-2-debuginfo-32bit-6.8.9.8-21.1
libMagickWand-6_Q16-2-debuginfo-32bit-6.8.9.8-21.1
ImageMagick-debuginfo-6.8.9.8-21.1
libMagick++-devel-32bit-6.8.9.8-21.1
libMagick++-6_Q16-5-32bit-6.8.9.8-21.1
ImageMagick-extra-debuginfo-6.8.9.8-21.1
libMagickWand-6_Q16-2-6.8.9.8-21.1
libMagick++-devel-6.8.9.8-21.1
ImageMagick-devel-6.8.9.8-21.1
libMagickCore-6_Q16-2-6.8.9.8-21.1
libMagickCore-6_Q16-2-debuginfo-6.8.9.8-21.1
libMagick++-6_Q16-5-6.8.9.8-21.1
libMagick++-6_Q16-5-debuginfo-6.8.9.8-21.1

## 144669 - SuSE SLES 11 SP4 SUSE-SU-2016:1581-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9767, CVE-2015-4116, CVE-2015-7803, CVE-2015-8835, CVE-2015-8838, CVE-2015-8866, CVE-2015-8867, CVE-2015-8873, CVE-2015-8874, CVE-2015-8879, CVE-2016-2554, CVE-2016-3141, CVE-2016-3142, CVE-2016-3185, CVE-2016-4070, CVE-2016-4073, CVE-2016-4342, CVE-2016-4346, 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-2016-5095, CVE-2016-5096, CVE-2016-5114

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1581-1

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-June/002115.html

SuSE SLES 11 SP4
i586
php53-dom-5.3.17-71.1
php53-xmlwriter-5.3.17-71.1
php53-exif-5.3.17-71.1
php53-gmp-5.3.17-71.1
php53-curl-5.3.17-71.1
php53-sysvsem-5.3.17-71.1
php53-pcntl-5.3.17-71.1
php53-fastcgi-5.3.17-71.1
php53-5.3.17-71.1
php53-pgsql-5.3.17-71.1
php53-sysvmsg-5.3.17-71.1
php53-snmp-5.3.17-71.1
php53-mbstring-5.3.17-71.1
php53-tokenizer-5.3.17-71.1
apache2-mod_php53-5.3.17-71.1
php53-mcrypt-5.3.17-71.1
php53-gettext-5.3.17-71.1
php53-pear-5.3.17-71.1
php53-ftp-5.3.17-71.1
php53-iconv-5.3.17-71.1
php53-shmop-5.3.17-71.1
php53-mysql-5.3.17-71.1
php53-xmlreader-5.3.17-71.1
php53-wddx-5.3.17-71.1
php53-fileinfo-5.3.17-71.1
php53-xmlrpc-5.3.17-71.1
php53-gd-5.3.17-71.1
php53-openssl-5.3.17-71.1
php53-ldap-5.3.17-71.1
php53-zlib-5.3.17-71.1
php53-dba-5.3.17-71.1
php53-pdo-5.3.17-71.1
php53-odbc-5.3.17-71.1
php53-intl-5.3.17-71.1
php53-zip-5.3.17-71.1
php53-sysvshm-5.3.17-71.1
php53-ctype-5.3.17-71.1

php53-json-5.3.17-71.1
php53-suhosin-5.3.17-71.1
php53-pspell-5.3.17-71.1
php53-bcmath-5.3.17-71.1
php53-xsl-5.3.17-71.1
php53-bz2-5.3.17-71.1
php53-calendar-5.3.17-71.1
php53-soap-5.3.17-71.1

x86_64
php53-dom-5.3.17-71.1
php53-xmlwriter-5.3.17-71.1
php53-exif-5.3.17-71.1
php53-gmp-5.3.17-71.1
php53-curl-5.3.17-71.1
php53-sysvsem-5.3.17-71.1
php53-pcntl-5.3.17-71.1
php53-fastcgi-5.3.17-71.1
php53-5.3.17-71.1
php53-pgsql-5.3.17-71.1
php53-sysvmsg-5.3.17-71.1
php53-snmp-5.3.17-71.1
php53-mbstring-5.3.17-71.1
php53-tokenizer-5.3.17-71.1
apache2-mod_php53-5.3.17-71.1
php53-mcrypt-5.3.17-71.1
php53-gettext-5.3.17-71.1
php53-pear-5.3.17-71.1
php53-ftp-5.3.17-71.1
php53-iconv-5.3.17-71.1
php53-shmop-5.3.17-71.1
php53-mysql-5.3.17-71.1
php53-xmlreader-5.3.17-71.1
php53-wddx-5.3.17-71.1
php53-fileinfo-5.3.17-71.1
php53-xmlrpc-5.3.17-71.1
php53-gd-5.3.17-71.1
php53-openssl-5.3.17-71.1
php53-ldap-5.3.17-71.1
php53-zlib-5.3.17-71.1
php53-dba-5.3.17-71.1
php53-pdo-5.3.17-71.1
php53-odbc-5.3.17-71.1
php53-intl-5.3.17-71.1
php53-zip-5.3.17-71.1
php53-sysvshm-5.3.17-71.1
php53-ctype-5.3.17-71.1
php53-json-5.3.17-71.1
php53-suhosin-5.3.17-71.1
php53-pspell-5.3.17-71.1
php53-bcmath-5.3.17-71.1
php53-xsl-5.3.17-71.1
php53-bz2-5.3.17-71.1
php53-calendar-5.3.17-71.1
php53-soap-5.3.17-71.1

## 144670 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1538-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8806, CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-2073, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449, CVE-2016-4483

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1538-1

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-June/002104.html

SuSE SLED 12 SP1
x86_64
libxml2-tools-2.9.1-24.1
python-libxml2-debugsource-2.9.1-24.1
libxml2-2-32bit-2.9.1-24.1
libxml2-2-2.9.1-24.1
python-libxml2-debuginfo-2.9.1-24.1
libxml2-2-debuginfo-32bit-2.9.1-24.1
libxml2-debugsource-2.9.1-24.1
libxml2-2-debuginfo-2.9.1-24.1
libxml2-tools-debuginfo-2.9.1-24.1
python-libxml2-2.9.1-24.1

SuSE SLED 12
x86_64
libxml2-tools-2.9.1-24.1
python-libxml2-debugsource-2.9.1-24.1
libxml2-2-32bit-2.9.1-24.1
libxml2-2-2.9.1-24.1
python-libxml2-debuginfo-2.9.1-24.1
libxml2-2-debuginfo-32bit-2.9.1-24.1
libxml2-debugsource-2.9.1-24.1
libxml2-2-debuginfo-2.9.1-24.1
libxml2-tools-debuginfo-2.9.1-24.1
python-libxml2-2.9.1-24.1

SuSE SLES 12 SP1
noarch
libxml2-doc-2.9.1-24.1

x86_64
libxml2-tools-2.9.1-24.1
python-libxml2-debugsource-2.9.1-24.1
libxml2-tools-debuginfo-2.9.1-24.1
libxml2-2-2.9.1-24.1
python-libxml2-debuginfo-2.9.1-24.1
libxml2-2-32bit-2.9.1-24.1
libxml2-debugsource-2.9.1-24.1
libxml2-2-debuginfo-32bit-2.9.1-24.1
libxml2-2-debuginfo-2.9.1-24.1
python-libxml2-2.9.1-24.1

SuSE SLES 12
noarch
libxml2-doc-2.9.1-24.1

x86_64
libxml2-tools-2.9.1-24.1
python-libxml2-debugsource-2.9.1-24.1
libxml2-tools-debuginfo-2.9.1-24.1
libxml2-2-2.9.1-24.1
python-libxml2-debuginfo-2.9.1-24.1
libxml2-2-32bit-2.9.1-24.1
libxml2-debugsource-2.9.1-24.1
libxml2-2-debuginfo-32bit-2.9.1-24.1
libxml2-2-debuginfo-2.9.1-24.1
python-libxml2-2.9.1-24.1

## 144671 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1561-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0749, CVE-2016-2150

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1561-1

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-June/002110.html

SuSE SLED 12
x86_64
libspice-server1-0.12.4-8.9.1
spice-debugsource-0.12.4-8.9.1
libspice-server1-debuginfo-0.12.4-8.9.1

SuSE SLES 12
x86_64
libspice-server1-0.12.4-8.9.1
spice-debugsource-0.12.4-8.9.1
libspice-server1-debuginfo-0.12.4-8.9.1

## 144677 - SuSE Linux 13.1 openSUSE-SU-2016:1558-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3125

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1558-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00045.html

SuSE Linux 13.1
i586
proftpd-debuginfo-1.3.5b-10.1
proftpd-doc-1.3.5b-10.1
proftpd-sqlite-debuginfo-1.3.5b-10.1
proftpd-sqlite-1.3.5b-10.1
proftpd-ldap-1.3.5b-10.1
proftpd-radius-debuginfo-1.3.5b-10.1
proftpd-debugsource-1.3.5b-10.1
proftpd-1.3.5b-10.1
proftpd-radius-1.3.5b-10.1
proftpd-mysql-debuginfo-1.3.5b-10.1
proftpd-devel-1.3.5b-10.1
proftpd-mysql-1.3.5b-10.1
proftpd-pgsql-1.3.5b-10.1
proftpd-pgsql-debuginfo-1.3.5b-10.1
proftpd-ldap-debuginfo-1.3.5b-10.1

noarch
proftpd-lang-1.3.5b-10.1

x86_64
proftpd-debuginfo-1.3.5b-10.1
proftpd-doc-1.3.5b-10.1
proftpd-sqlite-debuginfo-1.3.5b-10.1
proftpd-sqlite-1.3.5b-10.1
proftpd-ldap-1.3.5b-10.1
proftpd-radius-debuginfo-1.3.5b-10.1
proftpd-debugsource-1.3.5b-10.1
proftpd-1.3.5b-10.1
proftpd-radius-1.3.5b-10.1
proftpd-mysql-debuginfo-1.3.5b-10.1
proftpd-devel-1.3.5b-10.1
proftpd-mysql-1.3.5b-10.1
proftpd-pgsql-1.3.5b-10.1
proftpd-pgsql-debuginfo-1.3.5b-10.1
proftpd-ldap-debuginfo-1.3.5b-10.1

## 144680 - SuSE Linux 13.2 openSUSE-SU-2016:1522-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5118

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1522-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00025.html

SuSE Linux 13.2
x86_64
GraphicsMagick-debuginfo-1.3.20-6.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-6.1

libGraphicsMagick3-config-1.3.20-6.1
libGraphicsMagick++-devel-1.3.20-6.1
perl-GraphicsMagick-debuginfo-1.3.20-6.1
perl-GraphicsMagick-1.3.20-6.1
libGraphicsMagickWand-Q16-2-1.3.20-6.1
GraphicsMagick-devel-1.3.20-6.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-6.1
libGraphicsMagick-Q16-3-1.3.20-6.1
libGraphicsMagick-Q16-3-debuginfo-1.3.20-6.1
libGraphicsMagick++-Q16-3-1.3.20-6.1
GraphicsMagick-1.3.20-6.1
GraphicsMagick-debugsource-1.3.20-6.1

i586
GraphicsMagick-debuginfo-1.3.20-6.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.20-6.1
libGraphicsMagick3-config-1.3.20-6.1
libGraphicsMagick++-devel-1.3.20-6.1
perl-GraphicsMagick-debuginfo-1.3.20-6.1
perl-GraphicsMagick-1.3.20-6.1
libGraphicsMagickWand-Q16-2-1.3.20-6.1
GraphicsMagick-devel-1.3.20-6.1
libGraphicsMagick++-Q16-3-debuginfo-1.3.20-6.1
libGraphicsMagick-Q16-3-1.3.20-6.1
libGraphicsMagick-Q16-3-debuginfo-1.3.20-6.1
libGraphicsMagick++-Q16-3-1.3.20-6.1
GraphicsMagick-1.3.20-6.1
GraphicsMagick-debugsource-1.3.20-6.1

## 144682 - SuSE Linux 13.2 openSUSE-SU-2016:1566-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-2105, CVE-2016-2107

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1566-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00046.html

SuSE Linux 13.2
i586
nodejs-4.4.5-18.1
nodejs-devel-4.4.5-18.1
nodejs-debuginfo-4.4.5-18.1
nodejs-debugsource-4.4.5-18.1

noarch
nodejs-doc-4.4.5-18.1

x86_64
nodejs-4.4.5-18.1
nodejs-devel-4.4.5-18.1

nodejs-debuginfo-4.4.5-18.1
nodejs-debugsource-4.4.5-18.1

## 174966 - Scientific Linux Security ERRATA Important: openssl on SL6.x i386/x86_64 (1606-2153)

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

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2842

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: openssl on SL6.x i386/x86_64 (1606-2153)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=2153

SL6
x86_64
openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

i386
openssl-static-1.0.1e-48.el6_8.1
openssl-debuginfo-1.0.1e-48.el6_8.1
openssl-devel-1.0.1e-48.el6_8.1
openssl-1.0.1e-48.el6_8.1
openssl-perl-1.0.1e-48.el6_8.1

## 174969 - Scientific Linux Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1606-3306)

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

Risk Level: High

CVE: CVE-2016-2805, CVE-2016-2807

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: thunderbird on SL6.x i386/x86_64 (1606-3306)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=3306

SL6
x86_64
thunderbird-debuginfo-38.8.0-2.el6_8
thunderbird-38.8.0-2.el6_8

i386

thunderbird-debuginfo-38.8.0-2.el6_8
thunderbird-38.8.0-2.el6_8

## 20131 - (HPSBMU03575) HP Smart Update Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-0705, CVE-2016-0799, CVE-2016-0800, CVE-2016-2842

Description

Multiple vulnerabilities are present in some versions of HP Smart Update Manager.

Observation

HP Smart Update Manager is an installing and updating manager for HP products.

Multiple vulnerabilities are present in some versions of HP Smart Update Manager. The flaws lie in the OpenSSL library. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

## 20195 - Apache Struts REST Plugin Remote Code Execution

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

Risk Level: High

CVE: CVE-2016-3087

Description

A vulnerability in some versions of Apache Struts could lead to remote code execution.

Observation

A vulnerability in some versions of Apache Struts could lead to remote code execution.

The flaw lies in the handling of a crafted expression. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 20203 - Mozilla Firefox Multiple Vulnerabilities Prior To 47

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

Risk Level: High

CVE: CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2825, CVE-2016-2826, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833, CVE-2016-2834

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, to escalate privileges, to cause a denial of service condition or to bypass security measures.

## 20204 - Mozilla Firefox Multiple Vulnerabilities Prior To 47

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2825, CVE-2016-2826, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833, CVE-2016-2834

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, to escalate privileges, to cause a denial of service condition or to bypass security measures.

## 20208 - (APSB16-23) Vulnerability In Adobe AIR

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

Risk Level: High

CVE: CVE-2016-4126

Description

A vulnerability is present in some versions of Adobe AIR.

Observation

Adobe AIR is a cross-platform runtime environment that allows rich internet applications to be run on the desktop.

A vulnerability is present in some versions of Adobe AIR. The flaw lies in the directory search path used by the AIR installer. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB16-23 resolves this issue. The target system appears to be missing this update.

## 20209 - (APSB16-23) Vulnerability In Adobe AIR

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4126

Description

A vulnerability is present in some versions of Adobe AIR.

Observation

Adobe AIR is a cross-platform runtime environment that allows rich internet applications to be run on the desktop.

A vulnerability is present in some versions of Adobe AIR. The flaw lies in the directory search path used by the AIR installer. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB16-23 resolves this issue. The target system appears to be missing this update.

## 144662 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1543-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1543-1

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-June/002106.html

SuSE SLED 12 SP1
x86_64
poppler-tools-0.24.4-12.1
libpoppler44-0.24.4-12.1
poppler-debugsource-0.24.4-12.1
poppler-qt-debugsource-0.24.4-12.1
libpoppler-glib8-0.24.4-12.1
libpoppler-qt4-4-debuginfo-0.24.4-12.1
libpoppler-glib8-debuginfo-0.24.4-12.1
libpoppler-qt4-4-0.24.4-12.1
poppler-tools-debuginfo-0.24.4-12.1
libpoppler44-debuginfo-0.24.4-12.1

SuSE SLED 12
x86_64
poppler-tools-0.24.4-12.1
libpoppler44-0.24.4-12.1
poppler-debugsource-0.24.4-12.1
poppler-qt-debugsource-0.24.4-12.1
libpoppler-glib8-0.24.4-12.1
libpoppler-qt4-4-debuginfo-0.24.4-12.1
libpoppler-glib8-debuginfo-0.24.4-12.1
libpoppler-qt4-4-0.24.4-12.1
poppler-tools-debuginfo-0.24.4-12.1
libpoppler44-debuginfo-0.24.4-12.1

SuSE SLES 12 SP1
x86_64
poppler-tools-0.24.4-12.1
libpoppler44-0.24.4-12.1
poppler-debugsource-0.24.4-12.1
poppler-qt-debugsource-0.24.4-12.1
libpoppler-glib8-0.24.4-12.1
libpoppler-qt4-4-debuginfo-0.24.4-12.1
libpoppler-glib8-debuginfo-0.24.4-12.1
libpoppler-qt4-4-0.24.4-12.1
poppler-tools-debuginfo-0.24.4-12.1
libpoppler44-debuginfo-0.24.4-12.1

SuSE SLES 12
x86_64
poppler-tools-0.24.4-12.1
libpoppler44-0.24.4-12.1
poppler-debugsource-0.24.4-12.1
poppler-qt-debugsource-0.24.4-12.1
libpoppler-glib8-0.24.4-12.1

libpoppler-qt4-4-debuginfo-0.24.4-12.1
libpoppler-glib8-debuginfo-0.24.4-12.1
libpoppler-qt4-4-0.24.4-12.1
poppler-tools-debuginfo-0.24.4-12.1
libpoppler44-debuginfo-0.24.4-12.1

## 144664 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1560-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-3615, CVE-2014-3689, CVE-2014-9718, CVE-2015-3214, CVE-2015-5239, CVE-2015-5745, CVE-2015-7295, CVE-2015-7549, CVE-2015-8504, CVE-2015-8558, CVE-2015-8567, CVE-2015-8568, CVE-2015-8613, CVE-2015-8619, CVE-2015-8743, CVE-2015-8744, CVE-2015-8745, CVE-2015-8817, CVE-2015-8818, CVE-2016-1568, CVE-2016-1714, CVE-2016-1922, CVE-2016-1981, CVE-2016-2198, CVE-2016-2538, CVE-2016-2841, CVE-2016-2857, CVE-2016-2858, CVE-2016-3710, CVE-2016-3712, CVE-2016-4001, CVE-2016-4002, CVE-2016-4020, CVE-2016-4037, CVE-2016-4439, CVE-2016-4441, CVE-2016-4952

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1560-1

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-June/002109.html

SuSE SLED 12
x86_64
qemu-block-curl-2.0.2-48.19.1
qemu-x86-debuginfo-2.0.2-48.19.1
qemu-x86-2.0.2-48.19.1
qemu-block-curl-debuginfo-2.0.2-48.19.1
qemu-kvm-2.0.2-48.19.1
qemu-tools-debuginfo-2.0.2-48.19.1
qemu-tools-2.0.2-48.19.1
qemu-debugsource-2.0.2-48.19.1
qemu-2.0.2-48.19.1

noarch
qemu-sgabios-8-48.19.1
qemu-vgabios-1.7.4-48.19.1
qemu-ipxe-1.0.0-48.19.1
qemu-seabios-1.7.4-48.19.1

SuSE SLES 12
noarch
qemu-sgabios-8-48.19.1
qemu-vgabios-1.7.4-48.19.1
qemu-ipxe-1.0.0-48.19.1
qemu-seabios-1.7.4-48.19.1

x86_64
qemu-block-rbd-debuginfo-2.0.2-48.19.1
qemu-guest-agent-2.0.2-48.19.1
qemu-block-rbd-2.0.2-48.19.1
qemu-guest-agent-debuginfo-2.0.2-48.19.1
qemu-kvm-2.0.2-48.19.1
qemu-tools-2.0.2-48.19.1

qemu-lang-2.0.2-48.19.1
qemu-x86-2.0.2-48.19.1
qemu-2.0.2-48.19.1
qemu-block-curl-2.0.2-48.19.1
qemu-block-curl-debuginfo-2.0.2-48.19.1
qemu-x86-debuginfo-2.0.2-48.19.1
qemu-tools-debuginfo-2.0.2-48.19.1
qemu-debugsource-2.0.2-48.19.1

## 144679 - SuSE SLES 11 SP4 SUSE-SU-2016:1544-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1544-1

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-June/002107.html

SuSE SLES 11 SP4
i586
libpoppler-qt4-3-0.12.3-1.12.1
libpoppler-glib4-0.12.3-1.12.1
libpoppler5-0.12.3-1.12.1
poppler-tools-0.12.3-1.12.1

x86_64
libpoppler-qt4-3-0.12.3-1.12.1
libpoppler-glib4-0.12.3-1.12.1
libpoppler5-0.12.3-1.12.1
poppler-tools-0.12.3-1.12.1

## 185318 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2993-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2825, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833, CVE-2016-2834

Description

The scan detected that the host is missing the following update:
USN-2993-1

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-June/003451.html

Ubuntu 12.04

firefox_47.0+build3-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_47.0+build3-0ubuntu0.16.04.1

Ubuntu 15.10

firefox_47.0+build3-0ubuntu0.15.10.1

Ubuntu 14.04

firefox_47.0+build3-0ubuntu0.14.04.1

## 185309 - Ubuntu Linux 15.10 USN-3004-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3004-1

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-June/003461.html

Ubuntu 15.10

linux-image-4.2.0-1031-raspi2_4.2.0-1031.41

## 185310 - Ubuntu Linux 15.10 USN-3003-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3003-1

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-June/003460.html

Ubuntu 15.10

linux-image-4.2.0-38-generic_4.2.0-38.45

linux-image-4.2.0-38-generic-lpae_4.2.0-38.45
linux-image-4.2.0-38-powerpc-smp_4.2.0-38.45
linux-image-4.2.0-38-powerpc64-emb_4.2.0-38.45
linux-image-4.2.0-38-powerpc64-smp_4.2.0-38.45
linux-image-4.2.0-38-lowlatency_4.2.0-38.45
linux-image-4.2.0-38-powerpc-e500mc_4.2.0-38.45

## 185311 - Ubuntu Linux 14.04 USN-3002-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3002-1

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-June/003459.html

Ubuntu 14.04

linux-image-4.2.0-38-powerpc64-emb_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-powerpc-e500mc_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-generic_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-lowlatency_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-powerpc64-smp_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-powerpc-smp_4.2.0-38.45~14.04.1
linux-image-4.2.0-38-generic-lpae_4.2.0-38.45~14.04.1

## 185316 - Ubuntu Linux 12.04 USN-2998-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2069, CVE-2016-2117, CVE-2016-2187, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-4485, CVE-2016-4486, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-2998-1

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-June/003455.html

Ubuntu 12.04

linux-image-3.13.0-88-generic-lpae_3.13.0-88.135~precise1
linux-image-3.13.0-88-generic_3.13.0-88.135~precise1

## 185317 - Ubuntu Linux 14.04 USN-3001-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3001-1

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-June/003458.html

Ubuntu 14.04

linux-image-3.19.0-61-powerpc64-emb_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-powerpc-smp_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-powerpc64-smp_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-generic_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-generic-lpae_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-powerpc-e500mc_3.19.0-61.69~14.04.1
linux-image-3.19.0-61-lowlatency_3.19.0-61.69~14.04.1

## 185322 - Ubuntu Linux 14.04 USN-3000-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4004, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3136, CVE-2016-3137, CVE-2016-3140, CVE-2016-3672, CVE-2016-3689, CVE-2016-3951, CVE-2016-3955, CVE-2016-4485, CVE-2016-4486, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3000-1

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-June/003457.html

Ubuntu 14.04

linux-image-3.16.0-73-powerpc-smp_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-powerpc64-emb_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-powerpc64-smp_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-generic_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-powerpc-e500mc_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-lowlatency_3.16.0-73.95~14.04.1
linux-image-3.16.0-73-generic-lpae_3.16.0-73.95~14.04.1

## 20098 - (SYM16-006) Symantec Endpoint Encryption Unquoted Service Path Local Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2015-8156

Description

A privilege escalation vulnerability is present in some versions of Symantec Endpoint Encryption.

Observation

Symantec Endpoint Encryption is a disk encryption software.

A privilege escalation vulnerability is present in some versions of Symantec Endpoint Encryption. The flaw lies in the EEDService deployed in this product. Successful exploitation could allow a local attacker to escalate privileges and probably execute arbitrary code.

## 20126 - (HPSBGN3547) HP Device Manager Remote Read Access To Arbitrary Files Vulnerability

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

Risk Level: High

CVE: CVE-2011-4722

Description

An information disclosure vulnerability is present in some versions of HP Device Manager.

Observation

HP Device Manager is enterprise-class thin client management software.

An information disclosure vulnerability is present in some versions of HP Device Manager. The flaw lies in TFTP Server component. Successful exploitation could allow an attacker to read arbitrary files.

## 20194 - Wireshark Multiple Vulnerabilities Prior To 1.12.12

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a popular network protocol analyzer.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple components. Successful exploitation could allow an attacker to crash the application.

## 37525 - IBM AIX IV84269 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV84269

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV84269

5300-12
bos.net.tcp.client < 5.3.12.11

## 37526 - IBM AIX IV83984 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83984

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83984

6100-09
bos.net.tcp.client < 6.1.9.103

## 37527 - IBM AIX IV83993 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83993

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83993

7100-03
bos.net.tcp.client < 7.1.3.48

## 37528 - IBM AIX IV83994 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83994

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83994

7100-04
bos.net.tcp.client < 7.1.4.2

## 37529 - IBM AIX IV83995 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83995

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83995

7.2
bos.net.tcp.ntp < 7.2.0.3

## 37530 - IBM AIX IV83992 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83992

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83992

6100-09
ntp.rte < 6.1.9.103

## 37531 - IBM AIX IV83983 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7973, CVE-2015-7977, CVE-2015-7979, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158

Description

The scan detected that the host is missing the following update:
IV83983

Observation

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

http://www-01.ibm.com/support/docview.wss?uid=swg1IV83983

7.1
ntp.rte < 7.1.0.6

## 130518 - Debian Linux 8.0 DSA-3598-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5108

Description

The scan detected that the host is missing the following update:
DSA-3598-1

Observation

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

http://www.debian.org/security/2016/dsa-3598

Debian 8.0
all
vlc_2.2.4-1~deb8u1

## 130519 - Debian Linux 8.0 DSA-3602-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7456, CVE-2016-3074, 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-2016-5095, CVE-2016-5096

Description

The scan detected that the host is missing the following update:
DSA-3602-1

Observation

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

http://www.debian.org/security/2016/dsa-3602

Debian 8.0
all
php5_5.6.22+dfsg-0+deb8u1

## 144661 - SuSE SLES 11 SP4 SUSE-SU-2016:1528-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325, CVE-2016-1908, CVE-2016-3115

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1528-1

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-June/002103.html

SuSE SLES 11 SP4
i586
openssh-askpass-gnome-6.6p1-21.3
openssh-fips-6.6p1-21.1
openssh-helpers-6.6p1-21.1
openssh-6.6p1-21.1

x86_64
openssh-askpass-gnome-6.6p1-21.3
openssh-fips-6.6p1-21.1
openssh-helpers-6.6p1-21.1
openssh-6.6p1-21.1

## 144667 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1563-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-4957

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1563-1

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-June/002111.html

SuSE SLES 12 SP1
x86_64
ntp-4.2.8p8-14.1
ntp-debugsource-4.2.8p8-14.1
ntp-debuginfo-4.2.8p8-14.1

ntp-doc-4.2.8p8-14.1

SuSE SLED 12 SP1
x86_64
ntp-4.2.8p8-14.1
ntp-debugsource-4.2.8p8-14.1
ntp-debuginfo-4.2.8p8-14.1
ntp-doc-4.2.8p8-14.1

## 144672 - SuSE Linux 13.1 openSUSE-SU-2016:1556-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5097, CVE-2016-5098, CVE-2016-5099

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1556-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00043.html

SuSE Linux 13.1
noarch
phpMyAdmin-4.4.15.6-57.1

## 144673 - SuSE Linux 13.2 openSUSE-SU-2016:1553-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7456, CVE-2015-4116, CVE-2015-8873, CVE-2015-8874, CVE-2015-8876, CVE-2015-8877, CVE-2015-8879, CVE-2016-3074, CVE-2016-5093, CVE-2016-5094, CVE-2016-5095, CVE-2016-5096, CVE-2016-5114

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1553-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00040.html

SuSE Linux 13.2
i586
php5-tokenizer-debuginfo-5.6.1-66.1
php5-imap-5.6.1-66.1
php5-soap-5.6.1-66.1
php5-dom-debuginfo-5.6.1-66.1
php5-curl-debuginfo-5.6.1-66.1
php5-pcntl-debuginfo-5.6.1-66.1
php5-dom-5.6.1-66.1
php5-openssl-5.6.1-66.1

php5-snmp-5.6.1-66.1
php5-iconv-5.6.1-66.1
php5-gettext-debuginfo-5.6.1-66.1
php5-odbc-debuginfo-5.6.1-66.1
php5-tidy-debuginfo-5.6.1-66.1
php5-bcmath-debuginfo-5.6.1-66.1
php5-fileinfo-debuginfo-5.6.1-66.1
php5-firebird-5.6.1-66.1
php5-snmp-debuginfo-5.6.1-66.1
php5-fastcgi-debuginfo-5.6.1-66.1
php5-phar-5.6.1-66.1
php5-sqlite-debuginfo-5.6.1-66.1
php5-exif-5.6.1-66.1
php5-devel-5.6.1-66.1
php5-mcrypt-5.6.1-66.1
php5-posix-5.6.1-66.1
php5-ldap-debuginfo-5.6.1-66.1
php5-enchant-5.6.1-66.1
php5-calendar-5.6.1-66.1
apache2-mod_php5-debuginfo-5.6.1-66.1
php5-sqlite-5.6.1-66.1
php5-tidy-5.6.1-66.1
php5-sockets-debuginfo-5.6.1-66.1
php5-pgsql-debuginfo-5.6.1-66.1
php5-wddx-5.6.1-66.1
php5-fastcgi-5.6.1-66.1
php5-5.6.1-66.1
php5-xmlrpc-5.6.1-66.1
php5-enchant-debuginfo-5.6.1-66.1
php5-sysvmsg-5.6.1-66.1
php5-sysvshm-5.6.1-66.1
php5-zip-5.6.1-66.1
php5-readline-5.6.1-66.1
php5-pdo-5.6.1-66.1
php5-firebird-debuginfo-5.6.1-66.1
php5-calendar-debuginfo-5.6.1-66.1
php5-xmlreader-debuginfo-5.6.1-66.1
php5-xmlreader-5.6.1-66.1
php5-json-debuginfo-5.6.1-66.1
php5-gettext-5.6.1-66.1
php5-intl-5.6.1-66.1
php5-iconv-debuginfo-5.6.1-66.1
php5-openssl-debuginfo-5.6.1-66.1
php5-soap-debuginfo-5.6.1-66.1
php5-mssql-5.6.1-66.1
php5-curl-5.6.1-66.1
php5-sysvsem-debuginfo-5.6.1-66.1
php5-opcache-debuginfo-5.6.1-66.1
php5-bz2-5.6.1-66.1
php5-xsl-5.6.1-66.1
php5-odbc-5.6.1-66.1
php5-xmlwriter-5.6.1-66.1
php5-bcmath-5.6.1-66.1
php5-ctype-5.6.1-66.1
php5-posix-debuginfo-5.6.1-66.1
php5-dba-debuginfo-5.6.1-66.1
php5-dba-5.6.1-66.1
php5-ldap-5.6.1-66.1
php5-sockets-5.6.1-66.1
php5-ftp-debuginfo-5.6.1-66.1

php5-bz2-debuginfo-5.6.1-66.1
php5-zlib-debuginfo-5.6.1-66.1
php5-intl-debuginfo-5.6.1-66.1
php5-xmlrpc-debuginfo-5.6.1-66.1
php5-wddx-debuginfo-5.6.1-66.1
php5-sysvshm-debuginfo-5.6.1-66.1
php5-zip-debuginfo-5.6.1-66.1
php5-tokenizer-5.6.1-66.1
php5-sysvmsg-debuginfo-5.6.1-66.1
php5-shmop-5.6.1-66.1
php5-debugsource-5.6.1-66.1
php5-opcache-5.6.1-66.1
php5-mbstring-debuginfo-5.6.1-66.1
php5-readline-debuginfo-5.6.1-66.1
php5-mssql-debuginfo-5.6.1-66.1
php5-xmlwriter-debuginfo-5.6.1-66.1
php5-mysql-debuginfo-5.6.1-66.1
php5-sysvsem-5.6.1-66.1
php5-pgsql-5.6.1-66.1
php5-suhosin-debuginfo-5.6.1-66.1
php5-zlib-5.6.1-66.1
php5-mysql-5.6.1-66.1
php5-xsl-debuginfo-5.6.1-66.1
apache2-mod_php5-5.6.1-66.1
php5-pdo-debuginfo-5.6.1-66.1
php5-debuginfo-5.6.1-66.1
php5-fpm-5.6.1-66.1
php5-json-5.6.1-66.1
php5-gd-5.6.1-66.1
php5-suhosin-5.6.1-66.1
php5-exif-debuginfo-5.6.1-66.1
php5-shmop-debuginfo-5.6.1-66.1
php5-ctype-debuginfo-5.6.1-66.1
php5-mbstring-5.6.1-66.1
php5-pcntl-5.6.1-66.1
php5-phar-debuginfo-5.6.1-66.1
php5-gmp-debuginfo-5.6.1-66.1
php5-ftp-5.6.1-66.1
php5-mcrypt-debuginfo-5.6.1-66.1
php5-gd-debuginfo-5.6.1-66.1
php5-fileinfo-5.6.1-66.1
php5-imap-debuginfo-5.6.1-66.1
php5-pspell-debuginfo-5.6.1-66.1
php5-gmp-5.6.1-66.1
php5-fpm-debuginfo-5.6.1-66.1
php5-pspell-5.6.1-66.1

noarch
php5-pear-5.6.1-66.1

x86_64
php5-tokenizer-debuginfo-5.6.1-66.1
php5-imap-5.6.1-66.1
php5-soap-5.6.1-66.1
php5-dom-debuginfo-5.6.1-66.1
php5-curl-debuginfo-5.6.1-66.1
php5-pcntl-debuginfo-5.6.1-66.1
php5-dom-5.6.1-66.1
php5-openssl-5.6.1-66.1
php5-snmp-5.6.1-66.1

php5-iconv-5.6.1-66.1
php5-gettext-debuginfo-5.6.1-66.1
php5-odbc-debuginfo-5.6.1-66.1
php5-tidy-debuginfo-5.6.1-66.1
php5-bcmath-debuginfo-5.6.1-66.1
php5-fileinfo-debuginfo-5.6.1-66.1
php5-firebird-5.6.1-66.1
php5-snmp-debuginfo-5.6.1-66.1
php5-fastcgi-debuginfo-5.6.1-66.1
php5-phar-5.6.1-66.1
php5-sqlite-debuginfo-5.6.1-66.1
php5-exif-5.6.1-66.1
php5-devel-5.6.1-66.1
php5-mcrypt-5.6.1-66.1
php5-posix-5.6.1-66.1
php5-ldap-debuginfo-5.6.1-66.1
php5-enchant-5.6.1-66.1
php5-calendar-5.6.1-66.1
apache2-mod_php5-debuginfo-5.6.1-66.1
php5-sqlite-5.6.1-66.1
php5-tidy-5.6.1-66.1
php5-sockets-debuginfo-5.6.1-66.1
php5-pgsql-debuginfo-5.6.1-66.1
php5-wddx-5.6.1-66.1
php5-fastcgi-5.6.1-66.1
php5-5.6.1-66.1
php5-xmlrpc-5.6.1-66.1
php5-enchant-debuginfo-5.6.1-66.1
php5-sysvmsg-5.6.1-66.1
php5-sysvshm-5.6.1-66.1
php5-zip-5.6.1-66.1
php5-readline-5.6.1-66.1
php5-pdo-5.6.1-66.1
php5-firebird-debuginfo-5.6.1-66.1
php5-calendar-debuginfo-5.6.1-66.1
php5-xmlreader-debuginfo-5.6.1-66.1
php5-xmlreader-5.6.1-66.1
php5-json-debuginfo-5.6.1-66.1
php5-gettext-5.6.1-66.1
php5-intl-5.6.1-66.1
php5-iconv-debuginfo-5.6.1-66.1
php5-openssl-debuginfo-5.6.1-66.1
php5-soap-debuginfo-5.6.1-66.1
php5-mssql-5.6.1-66.1
php5-curl-5.6.1-66.1
php5-sysvsem-debuginfo-5.6.1-66.1
php5-opcache-debuginfo-5.6.1-66.1
php5-bz2-5.6.1-66.1
php5-xsl-5.6.1-66.1
php5-odbc-5.6.1-66.1
php5-xmlwriter-5.6.1-66.1
php5-bcmath-5.6.1-66.1
php5-ctype-5.6.1-66.1
php5-posix-debuginfo-5.6.1-66.1
php5-dba-debuginfo-5.6.1-66.1
php5-dba-5.6.1-66.1
php5-ldap-5.6.1-66.1
php5-sockets-5.6.1-66.1
php5-ftp-debuginfo-5.6.1-66.1
php5-bz2-debuginfo-5.6.1-66.1

php5-zlib-debuginfo-5.6.1-66.1
php5-intl-debuginfo-5.6.1-66.1
php5-xmlrpc-debuginfo-5.6.1-66.1
php5-wddx-debuginfo-5.6.1-66.1
php5-sysvshm-debuginfo-5.6.1-66.1
php5-zip-debuginfo-5.6.1-66.1
php5-tokenizer-5.6.1-66.1
php5-sysvmsg-debuginfo-5.6.1-66.1
php5-shmop-5.6.1-66.1
php5-debugsource-5.6.1-66.1
php5-opcache-5.6.1-66.1
php5-mbstring-debuginfo-5.6.1-66.1
php5-readline-debuginfo-5.6.1-66.1
php5-mssql-debuginfo-5.6.1-66.1
php5-xmlwriter-debuginfo-5.6.1-66.1
php5-mysql-debuginfo-5.6.1-66.1
php5-sysvsem-5.6.1-66.1
php5-pgsql-5.6.1-66.1
php5-suhosin-debuginfo-5.6.1-66.1
php5-zlib-5.6.1-66.1
php5-mysql-5.6.1-66.1
php5-xsl-debuginfo-5.6.1-66.1
apache2-mod_php5-5.6.1-66.1
php5-pdo-debuginfo-5.6.1-66.1
php5-debuginfo-5.6.1-66.1
php5-fpm-5.6.1-66.1
php5-json-5.6.1-66.1
php5-gd-5.6.1-66.1
php5-suhosin-5.6.1-66.1
php5-exif-debuginfo-5.6.1-66.1
php5-shmop-debuginfo-5.6.1-66.1
php5-ctype-debuginfo-5.6.1-66.1
php5-mbstring-5.6.1-66.1
php5-pcntl-5.6.1-66.1
php5-phar-debuginfo-5.6.1-66.1
php5-gmp-debuginfo-5.6.1-66.1
php5-ftp-5.6.1-66.1
php5-mcrypt-debuginfo-5.6.1-66.1
php5-gd-debuginfo-5.6.1-66.1
php5-fileinfo-5.6.1-66.1
php5-imap-debuginfo-5.6.1-66.1
php5-pspell-debuginfo-5.6.1-66.1
php5-gmp-5.6.1-66.1
php5-fpm-debuginfo-5.6.1-66.1
php5-pspell-5.6.1-66.1

## 144675 - SuSE Linux 13.2 openSUSE-SU-2016:1527-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1234, CVE-2016-3075, CVE-2016-3706, CVE-2016-4429

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1527-1

Observation

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

For more information see:

http://lists.opensuse.org/opensuse-updates/2016-06/msg00030.html

SuSE Linux 13.2
i586
glibc-obsolete-2.19-16.25.1
nscd-debuginfo-2.19-16.25.1
glibc-devel-2.19-16.25.1
glibc-devel-static-2.19-16.25.1
glibc-debugsource-2.19-16.25.1
glibc-locale-2.19-16.25.1
nscd-2.19-16.25.1
glibc-profile-2.19-16.25.1
glibc-debuginfo-2.19-16.25.1
glibc-devel-debuginfo-2.19-16.25.1
glibc-utils-debuginfo-2.19-16.25.1
glibc-extra-2.19-16.25.1
glibc-locale-debuginfo-2.19-16.25.1
glibc-utils-debugsource-2.19-16.25.1
glibc-obsolete-debuginfo-2.19-16.25.1
glibc-utils-2.19-16.25.1
glibc-2.19-16.25.1
glibc-extra-debuginfo-2.19-16.25.1

i686
glibc-profile-2.19-16.25.2
glibc-locale-debuginfo-2.19-16.25.2
glibc-debuginfo-2.19-16.25.2
glibc-devel-2.19-16.25.2
glibc-debugsource-2.19-16.25.2
glibc-locale-2.19-16.25.2
glibc-devel-static-2.19-16.25.2
glibc-2.19-16.25.2
glibc-devel-debuginfo-2.19-16.25.2

noarch
glibc-i18ndata-2.19-16.25.1
glibc-html-2.19-16.25.1
glibc-info-2.19-16.25.1

x86_64
glibc-locale-32bit-2.19-16.25.2
glibc-devel-static-32bit-2.19-16.25.2
nscd-debuginfo-2.19-16.25.1
glibc-devel-2.19-16.25.1
glibc-utils-32bit-2.19-16.25.1
glibc-devel-static-2.19-16.25.1
glibc-debugsource-2.19-16.25.1
glibc-32bit-2.19-16.25.2
glibc-locale-2.19-16.25.1
nscd-2.19-16.25.1
glibc-profile-2.19-16.25.1
glibc-debuginfo-2.19-16.25.1
glibc-devel-debuginfo-2.19-16.25.1
glibc-utils-debuginfo-2.19-16.25.1
glibc-extra-2.19-16.25.1
glibc-locale-debuginfo-32bit-2.19-16.25.2
glibc-utils-debuginfo-32bit-2.19-16.25.1
glibc-locale-debuginfo-2.19-16.25.1

glibc-utils-debugsource-2.19-16.25.1
glibc-devel-32bit-2.19-16.25.2
glibc-profile-32bit-2.19-16.25.2
glibc-debuginfo-32bit-2.19-16.25.2
glibc-devel-debuginfo-32bit-2.19-16.25.2
glibc-utils-2.19-16.25.1
glibc-2.19-16.25.1
glibc-extra-debuginfo-2.19-16.25.1

## 163103 - Oracle Enterprise Linux ELSA-2016-3573 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

Description

The scan detected that the host is missing the following update:
ELSA-2016-3573

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006110.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006111.html

OEL7
x86_64
kernel-uek-devel-3.8.13-118.7.1.el7uek
kernel-uek-debug-devel-3.8.13-118.7.1.el7uek
kernel-uek-doc-3.8.13-118.7.1.el7uek
kernel-uek-firmware-3.8.13-118.7.1.el7uek
kernel-uek-3.8.13-118.7.1.el7uek
kernel-uek-debug-3.8.13-118.7.1.el7uek
dtrace-modules-3.8.13-118.7.1.el7uek-0.4.5-3.el7

OEL6
x86_64
kernel-uek-debug-devel-3.8.13-118.7.1.el6uek
kernel-uek-devel-3.8.13-118.7.1.el6uek
kernel-uek-3.8.13-118.7.1.el6uek
kernel-uek-doc-3.8.13-118.7.1.el6uek
dtrace-modules-3.8.13-118.7.1.el6uek-0.4.5-3.el6
kernel-uek-firmware-3.8.13-118.7.1.el6uek
kernel-uek-debug-3.8.13-118.7.1.el6uek

## 163105 - Oracle Enterprise Linux ELSA-2016-3570 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

Description

The scan detected that the host is missing the following update:
ELSA-2016-3570

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006108.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006109.html

OEL7
x86_64
kernel-uek-firmware-4.1.12-37.5.1.el7uek
kernel-uek-4.1.12-37.5.1.el7uek
kernel-uek-debug-4.1.12-37.5.1.el7uek
kernel-uek-debug-devel-4.1.12-37.5.1.el7uek
dtrace-modules-4.1.12-37.5.1.el7uek-0.5.2-1.el7
kernel-uek-doc-4.1.12-37.5.1.el7uek
kernel-uek-devel-4.1.12-37.5.1.el7uek

OEL6
x86_64
dtrace-modules-4.1.12-37.5.1.el6uek-0.5.2-1.el6
kernel-uek-debug-devel-4.1.12-37.5.1.el6uek
kernel-uek-4.1.12-37.5.1.el6uek
kernel-uek-debug-4.1.12-37.5.1.el6uek
kernel-uek-devel-4.1.12-37.5.1.el6uek
kernel-uek-doc-4.1.12-37.5.1.el6uek
kernel-uek-firmware-4.1.12-37.5.1.el6uek

## 163106 - Oracle Enterprise Linux ELSA-2016-3572 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4565

Description

The scan detected that the host is missing the following update:
ELSA-2016-3572

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006113.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006112.html

OEL5
x86_64
kernel-uek-2.6.39-400.280.1.el5uek
kernel-uek-debug-devel-2.6.39-400.280.1.el5uek
kernel-uek-devel-2.6.39-400.280.1.el5uek
kernel-uek-doc-2.6.39-400.280.1.el5uek
kernel-uek-firmware-2.6.39-400.280.1.el5uek
kernel-uek-debug-2.6.39-400.280.1.el5uek

i386
kernel-uek-2.6.39-400.280.1.el5uek
kernel-uek-debug-devel-2.6.39-400.280.1.el5uek
kernel-uek-devel-2.6.39-400.280.1.el5uek
kernel-uek-doc-2.6.39-400.280.1.el5uek

kernel-uek-debug-2.6.39-400.280.1.el5uek
kernel-uek-firmware-2.6.39-400.280.1.el5uek

OEL6
x86_64
kernel-uek-doc-2.6.39-400.280.1.el6uek
kernel-uek-debug-2.6.39-400.280.1.el6uek
kernel-uek-2.6.39-400.280.1.el6uek
kernel-uek-debug-devel-2.6.39-400.280.1.el6uek
kernel-uek-firmware-2.6.39-400.280.1.el6uek
kernel-uek-devel-2.6.39-400.280.1.el6uek

i386
kernel-uek-doc-2.6.39-400.280.1.el6uek
kernel-uek-debug-2.6.39-400.280.1.el6uek
kernel-uek-2.6.39-400.280.1.el6uek
kernel-uek-debug-devel-2.6.39-400.280.1.el6uek
kernel-uek-firmware-2.6.39-400.280.1.el6uek
kernel-uek-devel-2.6.39-400.280.1.el6uek

## 174964 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1606-2582)

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

Risk Level: High

CVE: CVE-2016-3710

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1606-2582)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=2582

SL6
x86_64
qemu-kvm-tools-0.12.1.2-2.491.el6_8.1
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1
qemu-kvm-0.12.1.2-2.491.el6_8.1
qemu-img-0.12.1.2-2.491.el6_8.1

i386
qemu-guest-agent-0.12.1.2-2.491.el6_8.1
qemu-kvm-debuginfo-0.12.1.2-2.491.el6_8.1

## 174970 - Scientific Linux Security ERRATA Moderate: file on SL6.x i386/x86_64 (1606-850)

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

Risk Level: High

CVE: CVE-2014-3538, CVE-2014-3587, CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9620, CVE-2014-9653

Description

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

Security ERRATA Moderate: file on SL6.x i386/x86_64 (1606-850)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=850

SL6
x86_64
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

i386
file-libs-5.04-30.el6
file-5.04-30.el6
file-static-5.04-30.el6
file-debuginfo-5.04-30.el6
python-magic-5.04-30.el6
file-devel-5.04-30.el6

## 181970 - FreeBSD VLC Possibly Remote Code Execution Via Crafted File (6d402857-2fba-11e6-9f31-5404a68ad561)

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

Risk Level: High

CVE: CVE-2016-5108

Description

The scan detected that the host is missing the following update:
VLC -- Possibly remote code execution via crafted file (6d402857-2fba-11e6-9f31-5404a68ad561)

Observation

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

http://www.vuxml.org/freebsd/6d402857-2fba-11e6-9f31-5404a68ad561.html

Affected packages:
vlc < 2.2.4,4
vlc-qt4 < 2.2.4,4

## 185308 - Ubuntu Linux 12.04 USN-2997-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2187, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3955, CVE-2016-4485, CVE-2016-4486

Description

The scan detected that the host is missing the following update:
USN-2997-1

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-June/003454.html

Ubuntu 12.04

linux-image-3.2.0-1482-omap4_3.2.0-1482.109

## 185312 - Ubuntu Linux 16.04 USN-3007-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8839, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4558, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3007-1

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-June/003464.html

Ubuntu 16.04

linux-image-4.4.0-1012-raspi2_4.4.0-1012.16

## 185314 - Ubuntu Linux 16.04 USN-3006-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8839, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4558, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3006-1

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-June/003462.html

Ubuntu 16.04

linux-image-4.4.0-24-powerpc-smp_4.4.0-24.43
linux-image-4.4.0-24-generic-lpae_4.4.0-24.43
linux-image-4.4.0-24-powerpc64-smp_4.4.0-24.43
linux-image-4.4.0-24-powerpc-e500mc_4.4.0-24.43

linux-image-4.4.0-24-generic_4.4.0-24.43
linux-image-4.4.0-24-powerpc64-emb_4.4.0-24.43
linux-image-4.4.0-24-lowlatency_4.4.0-24.43

## 185319 - Ubuntu Linux 12.04 USN-2996-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1583, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2187, CVE-2016-2188, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3955, CVE-2016-4485, CVE-2016-4486

Description

The scan detected that the host is missing the following update:
USN-2996-1

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-June/003453.html

Ubuntu 12.04

linux-image-3.2.0-104-generic-pae_3.2.0-104.145
linux-image-3.2.0-104-virtual_3.2.0-104.145
linux-image-3.2.0-104-omap_3.2.0-104.145
linux-image-3.2.0-104-powerpc-smp_3.2.0-104.145
linux-image-3.2.0-104-generic_3.2.0-104.145
linux-image-3.2.0-104-powerpc64-smp_3.2.0-104.145
linux-image-3.2.0-104-highbank_3.2.0-104.145

## 185321 - Ubuntu Linux 14.04 USN-3005-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8839, CVE-2016-1583, CVE-2016-2117, CVE-2016-2187, CVE-2016-3961, CVE-2016-4485, CVE-2016-4486, CVE-2016-4558, CVE-2016-4565, CVE-2016-4581

Description

The scan detected that the host is missing the following update:
USN-3005-1

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-June/003463.html

Ubuntu 14.04

linux-image-4.4.0-24-powerpc-e500mc_4.4.0-24.43~14.04.1
linux-image-4.4.0-24-generic_4.4.0-24.43~14.04.1
linux-image-4.4.0-24-powerpc64-emb_4.4.0-24.43~14.04.1
linux-image-4.4.0-24-lowlatency_4.4.0-24.43~14.04.1
linux-image-4.4.0-24-generic-lpae_4.4.0-24.43~14.04.1

linux-image-4.4.0-24-powerpc-smp_4.4.0-24.43~14.04.1
linux-image-4.4.0-24-powerpc64-smp_4.4.0-24.43~14.04.1

### 130517 - Debian Linux 8.0 DSA-3599-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2335

Description

The scan detected that the host is missing the following update:
DSA-3599-1

Observation

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

http://www.debian.org/security/2016/dsa-3599

Debian 8.0
all
p7zip_9.20.1~dfsg.1-4.1+deb8u2

### 141209 - Red Hat Enterprise Linux RHSA-2016-1217 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2828, CVE-2016-2831

Description

The scan detected that the host is missing the following update:
RHSA-2016-1217

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2016-June/msg00006.html

RHEL5S
i386
firefox-debuginfo-45.2.0-1.el5_11
firefox-45.2.0-1.el5_11

x86_64
firefox-debuginfo-45.2.0-1.el5_11
firefox-45.2.0-1.el5_11

RHEL7S
x86_64
firefox-debuginfo-45.2.0-1.el7_2
firefox-45.2.0-1.el7_2

RHEL6S
i386
firefox-45.2.0-1.el6_8

firefox-debuginfo-45.2.0-1.el6_8

x86_64
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

RHEL6WS
x86_64
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

i386
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

RHEL5D
x86_64
firefox-debuginfo-45.2.0-1.el5_11
firefox-45.2.0-1.el5_11

i386
firefox-debuginfo-45.2.0-1.el5_11
firefox-45.2.0-1.el5_11

RHEL7D
x86_64
firefox-debuginfo-45.2.0-1.el7_2
firefox-45.2.0-1.el7_2

RHEL6D
x86_64
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

i386
firefox-45.2.0-1.el6_8
firefox-debuginfo-45.2.0-1.el6_8

RHEL7WS
x86_64
firefox-debuginfo-45.2.0-1.el7_2
firefox-45.2.0-1.el7_2

## 144668 - SuSE Linux 13.2 openSUSE-SU-2016:1552-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2825, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833, CVE-2016-2834

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1552-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00039.html

SuSE Linux 13.2
x86_64
MozillaFirefox-debugsource-47.0-71.1
mozilla-nss-tools-debuginfo-3.23-34.1
MozillaFirefox-buildsymbols-47.0-71.1
mozilla-nss-32bit-3.23-34.1
MozillaFirefox-translations-common-47.0-71.1
mozilla-nss-sysinit-3.23-34.1
mozilla-nss-certs-32bit-3.23-34.1
mozilla-nss-debuginfo-32bit-3.23-34.1
libsoftokn3-debuginfo-32bit-3.23-34.1
MozillaFirefox-translations-other-47.0-71.1
MozillaFirefox-devel-47.0-71.1
libfreebl3-debuginfo-32bit-3.23-34.1
libfreebl3-debuginfo-3.23-34.1
libfreebl3-3.23-34.1
mozilla-nss-certs-debuginfo-3.23-34.1
libfreebl3-32bit-3.23-34.1
mozilla-nss-debugsource-3.23-34.1
mozilla-nss-certs-debuginfo-32bit-3.23-34.1
libsoftokn3-32bit-3.23-34.1
mozilla-nss-sysinit-32bit-3.23-34.1
mozilla-nss-certs-3.23-34.1
MozillaFirefox-branding-upstream-47.0-71.1
MozillaFirefox-debuginfo-47.0-71.1
mozilla-nss-debuginfo-3.23-34.1
mozilla-nss-sysinit-debuginfo-3.23-34.1
libsoftokn3-3.23-34.1
MozillaFirefox-47.0-71.1
libsoftokn3-debuginfo-3.23-34.1
mozilla-nss-devel-3.23-34.1
mozilla-nss-3.23-34.1
mozilla-nss-tools-3.23-34.1
mozilla-nss-sysinit-debuginfo-32bit-3.23-34.1

i586
MozillaFirefox-buildsymbols-47.0-71.1
MozillaFirefox-47.0-71.1
mozilla-nss-sysinit-3.23-34.1
libfreebl3-3.23-34.1
mozilla-nss-3.23-34.1
MozillaFirefox-translations-common-47.0-71.1
mozilla-nss-tools-3.23-34.1
mozilla-nss-debuginfo-3.23-34.1
mozilla-nss-debugsource-3.23-34.1
MozillaFirefox-translations-other-47.0-71.1
mozilla-nss-devel-3.23-34.1
MozillaFirefox-debugsource-47.0-71.1
MozillaFirefox-devel-47.0-71.1
mozilla-nss-certs-debuginfo-3.23-34.1
libsoftokn3-debuginfo-3.23-34.1
libfreebl3-debuginfo-3.23-34.1
mozilla-nss-sysinit-debuginfo-3.23-34.1
mozilla-nss-certs-3.23-34.1
mozilla-nss-tools-debuginfo-3.23-34.1
MozillaFirefox-debuginfo-47.0-71.1
MozillaFirefox-branding-upstream-47.0-71.1
libsoftokn3-3.23-34.1

## 144678 - SuSE Linux 13.1 openSUSE-SU-2016:1557-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1950, CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2824, CVE-2016-2825, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833, CVE-2016-2834

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1557-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00044.html

SuSE Linux 13.1
x86_64
MozillaFirefox-47.0-116.1
mozilla-nss-32bit-3.23-80.1
MozillaFirefox-debuginfo-47.0-116.1
mozilla-nss-debuginfo-3.23-80.1
libfreebl3-debuginfo-32bit-3.23-80.1
mozilla-nss-sysinit-32bit-3.23-80.1
libsoftokn3-32bit-3.23-80.1
mozilla-nss-devel-3.23-80.1
mozilla-nss-sysinit-debuginfo-32bit-3.23-80.1
libfreebl3-3.23-80.1
libsoftokn3-debuginfo-32bit-3.23-80.1
MozillaFirefox-translations-other-47.0-116.1
mozilla-nss-certs-32bit-3.23-80.1
mozilla-nss-certs-debuginfo-32bit-3.23-80.1
mozilla-nss-debugsource-3.23-80.1
libfreebl3-32bit-3.23-80.1
MozillaFirefox-branding-upstream-47.0-116.1
mozilla-nss-sysinit-3.23-80.1
mozilla-nss-tools-3.23-80.1
mozilla-nss-debuginfo-32bit-3.23-80.1
MozillaFirefox-translations-common-47.0-116.1
mozilla-nss-certs-3.23-80.1
MozillaFirefox-debugsource-47.0-116.1
mozilla-nss-certs-debuginfo-3.23-80.1
mozilla-nss-3.23-80.1
libsoftokn3-debuginfo-3.23-80.1
mozilla-nss-sysinit-debuginfo-3.23-80.1
libfreebl3-debuginfo-3.23-80.1
libsoftokn3-3.23-80.1
MozillaFirefox-buildsymbols-47.0-116.1
mozilla-nss-tools-debuginfo-3.23-80.1
MozillaFirefox-devel-47.0-116.1

i586
MozillaFirefox-debuginfo-47.0-116.1
MozillaFirefox-debugsource-47.0-116.1
mozilla-nss-certs-debuginfo-3.23-80.1
MozillaFirefox-translations-other-47.0-116.1
mozilla-nss-debuginfo-3.23-80.1

MozillaFirefox-branding-upstream-47.0-116.1
mozilla-nss-sysinit-3.23-80.1
mozilla-nss-debugsource-3.23-80.1
mozilla-nss-devel-3.23-80.1
MozillaFirefox-translations-common-47.0-116.1
mozilla-nss-tools-3.23-80.1
mozilla-nss-certs-3.23-80.1
MozillaFirefox-47.0-116.1
libsoftokn3-debuginfo-3.23-80.1
libfreebl3-3.23-80.1
MozillaFirefox-devel-47.0-116.1
mozilla-nss-3.23-80.1
MozillaFirefox-buildsymbols-47.0-116.1
libfreebl3-debuginfo-3.23-80.1
mozilla-nss-tools-debuginfo-3.23-80.1
mozilla-nss-sysinit-debuginfo-3.23-80.1
libsoftokn3-3.23-80.1

## 163104 - Oracle Enterprise Linux ELSA-2016-1217 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2828, CVE-2016-2831

Description

The scan detected that the host is missing the following update:
ELSA-2016-1217

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-June/006107.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006106.html
http://oss.oracle.com/pipermail/el-errata/2016-June/006105.html

OEL6
x86_64
firefox-45.2.0-1.0.1.el6_8

i386
firefox-45.2.0-1.0.1.el6_8

OEL5
x86_64
firefox-45.2.0-1.0.1.el5_11

i386
firefox-45.2.0-1.0.1.el5_11

OEL7
x86_64
firefox-45.2.0-1.0.1.el7_2

## 174965 - Scientific Linux Security ERRATA Moderate: icedtea-web on SL6.x i386/x86_64 (1606-1796)

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

Risk Level: Medium

CVE: CVE-2015-5234, CVE-2015-5235

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: icedtea-web on SL6.x i386/x86_64 (1606-1796)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=1796

SL6
i386
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

noarch
icedtea-web-javadoc-1.6.2-1.el6

x86_64
icedtea-web-1.6.2-1.el6
icedtea-web-debuginfo-1.6.2-1.el6

## 174968 - Scientific Linux Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1606-2911)

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

Risk Level: Medium

CVE: CVE-2015-5352, CVE-2015-6563, CVE-2015-6564, CVE-2016-1908

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openssh on SL6.x i386/x86_64 (1606-2911)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=2911

SL6
x86_64
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6
openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

i386
openssh-server-5.3p1-117.el6
pam_ssh_agent_auth-0.9.3-117.el6
openssh-clients-5.3p1-117.el6
openssh-5.3p1-117.el6
openssh-ldap-5.3p1-117.el6

openssh-askpass-5.3p1-117.el6
openssh-debuginfo-5.3p1-117.el6

### 185315 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2995-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3947, 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:
USN-2995-1

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-June/003452.html

Ubuntu 12.04

squid3_3.1.19-1ubuntu3.12.04.7
squid-cgi_3.1.19-1ubuntu3.12.04.7

Ubuntu 16.04

squid3_3.5.12-1ubuntu7.2
squid-cgi_3.5.12-1ubuntu7.2

Ubuntu 15.10

squid3_3.3.8-1ubuntu16.3
squid-cgi_3.3.8-1ubuntu16.3

Ubuntu 14.04

squid3_3.3.8-1ubuntu6.8
squid-cgi_3.3.8-1ubuntu6.8

### 20201 - IBM WebSphere MQ Queue Manager Heap Storage Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-0260

Description

A denial of service vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

A denial of service vulnerability is present in some versions of IBM WebSphere MQ. The flaw is due to heap storage not been deallocated by queue manager agents. Successful exploitation could allow an attacker to cause a denial of service condition.

## 144674 - SuSE Linux 13.2 openSUSE-SU-2016:1526-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-5104

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1526-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00029.html

SuSE Linux 13.2
x86_64
libimobiledevice-doc-1.1.6-2.3.1
imobiledevice-tools-1.1.6-2.3.1
libimobiledevice-debugsource-1.1.6-2.3.1
libusbmuxd2-32bit-1.0.9-2.3.1
libimobiledevice4-1.1.6-2.3.1
libimobiledevice4-debuginfo-32bit-1.1.6-2.3.1
iproxy-debuginfo-1.0.9-2.3.1
imobiledevice-tools-debuginfo-1.1.6-2.3.1
libusbmuxd2-debuginfo-1.0.9-2.3.1
libusbmuxd-debugsource-1.0.9-2.3.1
libusbmuxd-devel-1.0.9-2.3.1
python-imobiledevice-1.1.6-2.3.1
libusbmuxd2-debuginfo-32bit-1.0.9-2.3.1
iproxy-1.0.9-2.3.1
libimobiledevice4-32bit-1.1.6-2.3.1
libimobiledevice4-debuginfo-1.1.6-2.3.1
libusbmuxd2-1.0.9-2.3.1
libimobiledevice-devel-1.1.6-2.3.1
python-imobiledevice-debuginfo-1.1.6-2.3.1

i586
libimobiledevice-doc-1.1.6-2.3.1
imobiledevice-tools-1.1.6-2.3.1
libimobiledevice-debugsource-1.1.6-2.3.1
libimobiledevice4-1.1.6-2.3.1
iproxy-debuginfo-1.0.9-2.3.1
imobiledevice-tools-debuginfo-1.1.6-2.3.1
libusbmuxd2-debuginfo-1.0.9-2.3.1
libusbmuxd-debugsource-1.0.9-2.3.1
libusbmuxd-devel-1.0.9-2.3.1
python-imobiledevice-1.1.6-2.3.1
iproxy-1.0.9-2.3.1
libimobiledevice4-debuginfo-1.1.6-2.3.1
libusbmuxd2-1.0.9-2.3.1
libimobiledevice-devel-1.1.6-2.3.1
python-imobiledevice-debuginfo-1.1.6-2.3.1

## 174967 - Scientific Linux Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1606-1297)

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

Risk Level: Medium

CVE: CVE-2014-9750, CVE-2015-5194, CVE-2015-5195, CVE-2015-5219, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7852, CVE-2015-7977, CVE-2015-7978

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: ntp on SL6.x i386/x86_64 (1606-1297)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1606&L=scientific-linux-errata&F=&S=&P=1297

SL6
i386
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

noarch
ntp-doc-4.2.6p5-10.el6

x86_64
ntpdate-4.2.6p5-10.el6
ntp-4.2.6p5-10.el6
ntp-debuginfo-4.2.6p5-10.el6
ntp-perl-4.2.6p5-10.el6

## 181971 - FreeBSD botan Cryptographic Vulnerability (f771880c-31cf-11e6-8e82-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2014-9742

Description

The scan detected that the host is missing the following update:
botan -- cryptographic vulnerability (f771880c-31cf-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/f771880c-31cf-11e6-8e82-002590263bf5.html

Affected packages:
botan110 < 1.10.8

## 181973 - FreeBSD botan Multiple Vulnerabilities (ac0900df-31d0-11e6-8e82-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-7827, CVE-2016-2849

Description

The scan detected that the host is missing the following update:
botan -- multiple vulnerabilities (ac0900df-31d0-11e6-8e82-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/ac0900df-31d0-11e6-8e82-002590263bf5.html

Affected packages:
botan110 < 1.10.13

## 144681 - SuSE Linux 13.2 openSUSE-SU-2016:1567-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3622, CVE-2016-4008

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:1567-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-06/msg00047.html

SuSE Linux 13.2
x86_64
libtasn1-devel-32bit-3.7-2.7.1
libtasn1-6-debuginfo-3.7-2.7.1
libtasn1-debugsource-3.7-2.7.1
libtasn1-debuginfo-3.7-2.7.1
libtasn1-6-3.7-2.7.1
libtasn1-3.7-2.7.1
libtasn1-6-32bit-3.7-2.7.1
libtasn1-devel-3.7-2.7.1
libtasn1-6-debuginfo-32bit-3.7-2.7.1

i586
libtasn1-6-debuginfo-3.7-2.7.1
libtasn1-debugsource-3.7-2.7.1
libtasn1-debuginfo-3.7-2.7.1
libtasn1-6-3.7-2.7.1
libtasn1-3.7-2.7.1
libtasn1-devel-3.7-2.7.1

## 33346 - Oracle Solaris 149497-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
149497-02

Observation

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

https://getupdates.oracle.com/readme/149497-02

SunOS 5.10(x86): pppd patch

SOLARIS_10_x86

SUNWpppdu:11.10.0,REV=2005.01.21.16.34
SUNWpppdt:11.10.0,REV=2005.01.21.16.34

**33347 - Oracle Solaris 150437-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
150437-02

Observation

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

https://getupdates.oracle.com/readme/150437-02

SunOS 5.10(x86): wanboot server patch

SOLARIS_10_x86

SUNWwbsup:11.10.0,REV=2005.01.21.16.34

**33348 - Oracle Solaris 149496-02 Update Is Not Installed**

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
149496-02

Observation

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

https://getupdates.oracle.com/readme/149496-02

SunOS 5.10: pppd patch

SOLARIS_10

SUNWpppdu:11.10.0,REV=2005.01.21.15.53
SUNWpppdt:11.10.0,REV=2005.01.21.15.53

### 88784 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1 SSA:2016-165-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4971

Description

The scan detected that the host is missing the following update:
SSA:2016-165-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.532542

Slackware 14.0
x86_64
wget-1.18-x86_64-1

Slackware 13.0
x86_64
wget-1.18-x86_64-1

Slackware 13.1
x86_64
wget-1.18-x86_64-1

Slackware 14.1
x86_64
wget-1.18-x86_64-1

Slackware 13.37
x86_64
wget-1.18-x86_64-1

### 181969 - FreeBSD OpenSSL Vulnerability In DSA Signing (6f0529e2-2e82-11e6-b2ec-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-2178

Description

The scan detected that the host is missing the following update:
OpenSSL -- vulnerability in DSA signing (6f0529e2-2e82-11e6-b2ec-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/6f0529e2-2e82-11e6-b2ec-b499baebfeaf.html

Affected packages:
openssl < 1.0.2_13
libressl < 2.3.6
libressl-devel < 2.4.1

### 181972 - FreeBSD roundcube XSS Vulnerability (97e86d10-2ea7-11e6-ae88-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-5103

Description

The scan detected that the host is missing the following update:
roundcube -- XSS vulnerability (97e86d10-2ea7-11e6-ae88-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/97e86d10-2ea7-11e6-ae88-002590263bf5.html

Affected packages:
roundcube < 1.1.5_1,1

### 181974 - FreeBSD expat Multiple Vulnerabilities (c9c252f5-2def-11e6-ae88-002590263bf5)

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

Risk Level: Low

CVE: CVE-2012-6702, CVE-2016-5300

Description

The scan detected that the host is missing the following update:
expat -- multiple vulnerabilities (c9c252f5-2def-11e6-ae88-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/c9c252f5-2def-11e6-ae88-002590263bf5.html

Affected packages:
expat < 2.1.1_1

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

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

Risk Level: Low

CVE: CVE-2016-4303

Description

The scan detected that the host is missing the following update:
iperf3 -- buffer overflow (d6bbf2d8-2cfc-11e6-800b-080027468580)

Observation

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

http://www.vuxml.org/freebsd/d6bbf2d8-2cfc-11e6-800b-080027468580.html

Affected packages:
3.1 <= iperf3 < 3.1.3
3.0 <= iperf3 < 3.0.12

### 185313 - Ubuntu Linux 14.04 USN-2999-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
USN-2999-1

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-June/003456.html

Ubuntu 14.04

linux-image-3.13.0-88-powerpc64-smp_3.13.0-88.135
linux-image-3.13.0-88-powerpc-e500_3.13.0-88.135
linux-image-3.13.0-88-powerpc64-emb_3.13.0-88.135
linux-image-3.13.0-88-powerpc-smp_3.13.0-88.135
linux-image-3.13.0-88-generic_3.13.0-88.135
linux-image-3.13.0-88-lowlatency_3.13.0-88.135
linux-image-3.13.0-88-generic-lpae_3.13.0-88.135
linux-image-3.13.0-88-powerpc-e500mc_3.13.0-88.135

### 185320 - Ubuntu Linux 16.04 USN-3008-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1583

Description

The scan detected that the host is missing the following update:
USN-3008-1

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-June/003465.html

Ubuntu 16.04

linux-image-4.4.0-1015-snapdragon_4.4.0-1015.18

### 20193 - (HPSBGN03565) HPE Virtualization Performance Viewer Local Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2015-7872

Description

A denial of service vulnerability is present in some versions of HPE Virtualization Performance Viewer.

Observation

HPE Virtualization Performance Viewer is used for performance monitoring in virtualized environments.

A denial of service vulnerability is present in some versions of HPE Virtualization Performance Viewer. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition.

### 144676 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1568-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-7704, CVE-2015-7705, CVE-2015-7974, CVE-2016-1547, CVE-2016-1548, CVE-2016-1549, CVE-2016-1550, CVE-2016-1551, CVE-2016-2516, CVE-2016-2517, CVE-2016-2518, CVE-2016-2519, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-4957

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:1568-1

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-June/002112.html

SuSE SLED 12
x86_64
ntp-debugsource-4.2.8p8-46.8.1
ntp-debuginfo-4.2.8p8-46.8.1
ntp-doc-4.2.8p8-46.8.1
ntp-4.2.8p8-46.8.1

SuSE SLES 12
x86_64
ntp-debugsource-4.2.8p8-46.8.1
ntp-debuginfo-4.2.8p8-46.8.1
ntp-doc-4.2.8p8-46.8.1
ntp-4.2.8p8-46.8.1

## 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.

### 1914 - SSH RSAREF Buffer Overflow

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

CVE: CVE-1999-0834

Update Details

FASLScript is updated

### 181963 - FreeBSD NSS Multiple Vulnerabilities (32166082-53fa-41fa-b081-207e7a989a0a)

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

Risk Level: High

CVE: CVE-2016-2834

Update Details

Risk is updated

### 33116 - Oracle Solaris 150383-14 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

### 19558 - (SOL17518) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7871

Update Details

FASLScript is updated

### 33145 - Oracle Solaris 150401-38 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-0399, CVE-2013-3799, CVE-2013-5862, CVE-2013-5876, CVE-2014-4215, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441

Update Details

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

### 144612 - SuSE Linux 13.2 openSUSE-SU-2016:1335-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Update Details

Risk is updated

### 181968 - FreeBSD mozilla Multiple Vulnerabilities (8065d37b-8e7c-4707-a608-1b0a2b8509c3)

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

Risk Level: Medium

CVE: CVE-2016-2815, CVE-2016-2818, CVE-2016-2819, CVE-2016-2821, CVE-2016-2822, CVE-2016-2825, CVE-2016-2828, CVE-2016-2829, CVE-2016-2831, CVE-2016-2832, CVE-2016-2833

Update Details

Risk is updated

### 190623 - Fedora Linux 24 FEDORA-2016-1c4e616564 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Update Details

Risk is updated

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

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7848

Update Details

FASLScript is updated

### 33146 - Oracle Solaris 148104-23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814

Update Details

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

### 33147 - Oracle Solaris 148105-23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2010-5107, CVE-2012-0814

Update Details

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

### 130502 - Debian Linux 8.0 DSA-3586-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4478

Update Details
Risk is updated

### 144601 - SuSE Linux 13.2 openSUSE-SU-2016:1314-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4414

Update Details
Risk is updated

### 144609 - SuSE Linux 13.2 openSUSE-SU-2016:1312-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-9773, CVE-2016-4478

Update Details
Risk is updated

### 190595 - Fedora Linux 24 FEDORA-2016-bf916bcc04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4414

Update Details
Risk is updated

### 190599 - Fedora Linux 23 FEDORA-2016-42f30d76a0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4414

Update Details
Risk is updated

### 190609 - Fedora Linux 22 FEDORA-2016-0431acaa78 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-4414

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7850

Update Details

FASLScript is updated

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

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7691, CVE-2015-7692, CVE-2015-7702

Update Details

FASLScript is updated

### 19483 - (SOL17525) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7853

Update Details

FASLScript is updated

### 19586 - (SOL02360853) F5 BIG-IP NTP Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-5194, CVE-2015-5195

Update Details

FASLScript is updated

### 33162 - Oracle Solaris 150400-38 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441

Update Details

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

### 70080 - random.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

### 70087 - hp.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

### 70109 - symantec.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

## HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

## MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.